An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Twentieth Annual Report of the Data Protection Commissioner 2008

Presented to each of the Houses of the Oireachtas pursuant to section 14 of the Data Protection Acts 1988 & 2003.

PRN. A9/0327

Contents

List of tables and figures

Part 1

Foreword

2008 was the year of data security. Lapses in both the public and private sectors led to significant losses of personal data. Some of these losses were reported in the media. There was heightened concern about the general quality of data security in this country. The question was increasingly asked: can we trust organisations to guard the personal data that we provide to them?

The response to the challenge has been encouraging. In the public sector, it has led to the issuance of new guidelines by the Department of Finance. These emphasise the responsibilities of State agencies to safeguard the personal data entrusted to them. They give practical advice on how this can be achieved.

There is an increasing recognition that proper handling of personal data is also a matter of good customer service. If customers cannot trust the State or private companies to treat their personal information with respect, they will be increasingly reluctant to part with such information.

My Office's activities during the year also had a heavy data security focus. We worked with the Department of Finance on the new public service guidelines. Our audit work had a significant focus on security. This is reflected in the new audit resource that we made available to organisations earlier this year. We were also in receipt of an increasing number of voluntary reports of data security breaches. We were able to help the organisations concerned to respond appropriately to these breaches. Often this led to a more fundamental review of data handling practices within organisations. Security also featured in the steady stream of complaints we had to deal with in the course of the year.

The question of whether reporting of data breaches should be a legal requirement is now being examined by a group set up by the Minister for Justice, Equality and Law Reform of which I am a member. The work of the group will take account of

developments at European Union level – in particular the likely requirement for data breach notification to be included in the revised *E*-Privacy Directive.

There is no room for complacency. Positive developments on technical aspects of data security have to be balanced against rather more worrying moves which could fatally undermine it. I have been particularly concerned at an apparent failure to recognise the need for greater care in the use of the PPSN (Personal Public Service Number). My concerns are set out in detail in the Report. The extended requirement to retain telecommunications data for possible police use, in accordance with the EU Data Retention Directive, also gives rise to security concerns – as well as more fundamental privacy issues.

As we face into a period of reduced resources, I want to pay tribute to the staff of the Office who continue to deliver a high quality of service across the full range of our responsibilities.

Billy Hawkes
Data Protection Commissioner
Portarlington, April 2009

Top Ten Threats to Privacy

Last year we decided to publish the top ten threats to individual privacy as identified by our staff and undertook to revisit the issue this year. This unscientific list represents my staff's perception of the major threats to privacy at the close of 2008, based on the queries and issues they deal with on a day to day basis.

1) Failure of organisations to have even the most basic protocols in place to minimise the loss of customer and employee data.

2) Continued lack of proper procedures in public and private sector bodies to limit access by their employees to our personal data on a 'need to know' basis.

3) Failure to take due account of the legitimate privacy expectations of members of the public when moving towards greater efficiency of public services. However, I am hopeful that developments in this area will be balanced.

4) The tendency of new legislation to seek ever more personal data from the public and the sharing of that data between organisations without (in many cases) any real business case to justify such sharing.

5) Criminals using increasingly sophisticated methods to part individuals from their personal data for criminal and fraudulent use.

6) The extended use of the Personal Public Service Number (PPSN). This is the number given to each one of us by the Government to identify us when we interact with public bodies. More and more services seek to use this identifying number, often without any credible justification.

7) Publication and availability of excessive personal data on the internet (sometimes placed there by the individuals themselves on social networking sites etc).

8) Continued lack of awareness among data controllers of their data protection obligations.

9) Indifference on the part of data controllers to the consequences of their actions when they deliberately and persistently refuse to respect the data protection rights of their customers.

10) Continued lack of awareness on the part of members of the general public (who, as a result, give away their personal information too easily, don't ask why personal information is needed or fail to 'tick the box' to say that we don't want to be contacted).

Introduction

The data protection agenda continues to be challenging and varied. As a result of the prevalence and necessity of personal data in all aspects of economic and social life, the Office of the Data Protection Commissioner finds itself called upon to offer views, give advice, and deal with complaints in relation to every aspect of life in Ireland. This ensures that the issues faced by the Office will always be fresh and challenging as we attempt to perform our functions to the best of our abilities and within the resources available to us.

The use of personal data is so widespread in our society that it is sometimes taken for granted by those bodies that are legally responsible for that data. We refer to these entities as 'data controllers'. This tendency to take our data for granted may be understandable if the data controller is not principally focused on personal data or if the data controller is not large enough to employ someone to deal with data protection obligations on a full time basis. Of course, ignorance of these obligations is not a legitimate excuse, especially given that data protection obligations are often simply a matter of good manners. There should be nothing strange about the obligation to ask someone's permission to use their personal data. It belongs to them; if you wish to use it, you should ask permission.

We entrust our personal data to organisations for good and practical reasons. We hand it over to receive medical, financial, educational and other services. We pass it to our employers, to our local and national authorities, to communications companies and to a host of other bodies. Sometimes we don't even have a choice about handing it over. There is also a desire to share this information between these bodies. They want the services they provide to be more efficient, to be less expensive, to be more coherent, and to be more integrated. They want their databases, full of once unimaginable quantities of our personal information, to be able to 'talk' to each other so that everyone is in the loop and opportunities are not missed.

What would happen if we stopped trusting them?

What would happen if the general public gradually became less trusting and began to resist handing over personal data?

A collapse of public trust in data-dependent services organisations would be hugely damaging. It would carry a hefty economic price-tag as we would be less competitive and less attractive as a market. The social consequences would arguably be worse. Our public administration would be hopelessly hamstrung. More people would fall through the gaps in our social services and fewer people would receive assistance when they need it.

But this will be regarded by many as idle conjecture. For such people, the idea that individual citizens will get fed up of their personal data being treated without due care is ridiculous. It seems to me as if sometimes the personal information of members of the public is seen as an inexhaustible resource, just like public confidence in service organisations.

Over the past year the general public have been reading, hearing and watching a steady stream of stories about breaches of data security. Typically a staff member leaves his or her office with a laptop containing records of thousands of unsuspecting clients or citizens that no one thought to encrypt. The laptop is stolen from a car, snatched on the street or left on a train. A company or public agency sends thousands of client details to the wrong clients because nobody thought to introduce regular checking. A junior employee downloads thousands of client records to an unencrypted USB memory key and loses it. Nobody thought to check what level of access the employee should have or even to train the employee about data protection responsibilities. A company sends unwanted direct marketing text messages to thousands of people because they weren't paying attention, didn't know the law or had technical problems. One story seems to follow another relentlessly.

If public and private sector organisations don't wake up to the damage they are doing to public confidence in their capacity to respect privacy, more than some awkward prosecutions by my Office may be at stake. Respect for privacy is part of the network of trust that our society relies upon. Privacy must be built into the foundations upon

which future developments are based. Data security is a vital building block for data sharing and without it members of the public will become wary of new developments.

The message is simple. Data protection is good for public administration and good for business. Data protection rules have been in place in this jurisdiction for twenty years. When all is said and done there can be no excuses for failing to respect them.

Customer Service

Customer service is at the heart of our mission as an Office. Most of what we do involves helping our customers to understand their data protection rights and obligations. Even when we investigate complaints, we seek to increase awareness of data protection rights and obligations among the organisations concerned. We are committed to providing the best possible service for them. We keep a tight focus on the provision of comprehensive, definitive and clear information and advice on all issues related to data protection. Our work to raise awareness of data protection rights often results in members of the public contacting us for more information. Our customers can obtain the information they need on our website, www.dataprotection.ie, or by contacting us directly by email, telephone or letter. Last year we continued to respond to large numbers of phone calls from members of the public on a very broad range of issues, from access rights to registration obligations. Emails were the next most common source of queries with a smaller number of queries received by post. Our media profile continues to be a valuable and cost effective element of our awareness-raising efforts, as journalists are increasingly well-informed on issues of privacy and data protection (we dealt with some 200 media queries last year, showing a continued high level of interest in privacy issues). We are continuing our efforts to use innovative tools to reach more people and to inform them of their rights. In 2008, we launched a privacy competition on YouTube with assistance from Google. We were delighted to interact with a cohort of tech-savvy young citizens that can be difficult to engage on privacy issues. Building on the success of last year's competition, we have already launched the 2009 competition with the assistance of Google.

In 2008 we continued our practice of ensuring that every member of our team was involved in the provision of advice and information directly to our customers (both data subjects and data controllers).[1] This helps to keep us fresh and engaged and ensures that our advice remains up-to-date and relevant. During 2008 we also made a large number of presentations to organisations and networks about their data protection obligations. These gatherings provided valuable opportunities to discuss privacy issues in the context of new technologies, products and challenges. Details of our presentations are given at appendix 1 of this report. We will continue, in so far as our resources allow, to respond to requests to speak at appropriate events.

The Office continues its efforts to provide services to customers in both Irish and English and to ensure that key information is available on our Irish language website, www.cosantasonrai.ie. Our efforts in this regard were greatly aided by the willingness of staff to undertake training to improve their capacity as Gaeilge.

Complaints and Investigations

For the second year in a row I am reporting a significant volume of complaints to my Office. A total of 1,031 complaints were submitted in 2008 compared to a total of 1,037 complaints received in 2007. These figures are considerably higher than in recent years; we received 658 complaints in 2006 and 300 in 2005. The large number of complaints continues to place a huge workload on my Office's Investigation Unit. Figure 1 - Complaints received, concluded and outstandingillustrates the numbers of complaints received, concluded and outstanding in 2007 and 2008.

[1] 'Data controllers' are organisations that collect and hold personal data on individuals ('data subjects')

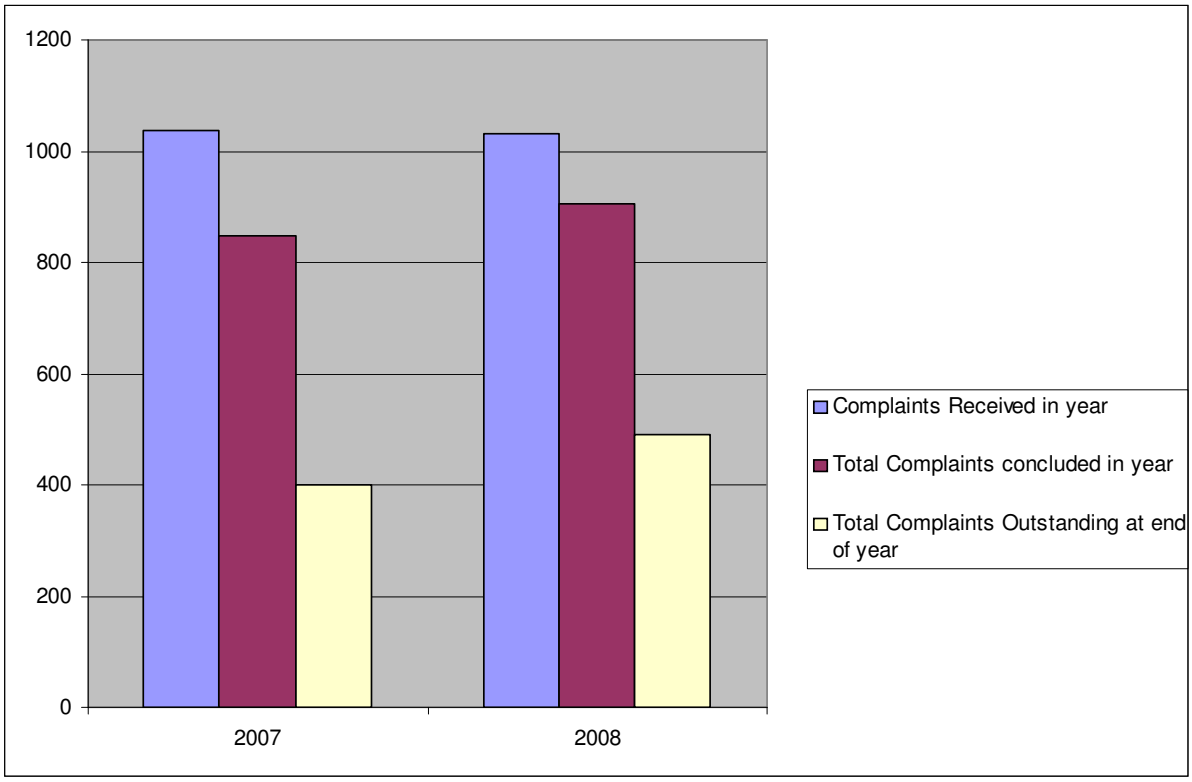

Figure 1 - Complaints received, concluded and outstanding

However, unlike last year there has been a significant and welcome decrease in the number of complaints which fall under the Privacy in Electronic Communications Regulations (S.I. 535 of 2003). In 2008 we received a total of 321 complaints in this category reporting unsolicited direct marketing text messages, phone calls, fax messages and emails. This compares with 538 such complaints in 2007. A number of factors are likely to have contributed to the decrease in this category of complaint. In regard to marketing phone calls and fax messages, those involved are more aware of legal requirements governing the use of phone numbers which are entered on the National Directory Database Opt-Out Register. In addition, the number of phone numbers entered on that Register continues to grow. As a result, complaints concerning cold calling are down considerably on previous years. Regarding unsolicited marketing text messages, my Office received almost 200 fewer complaints in 2008 than in 2007. I attribute this decrease to the effect on the text marketing sector of prosecution proceedings which I brought to the District Court towards the end of 2007 against a number of companies operating in that sector. At the time of writing those matters remain before the courts. However, it is clear that those sending such messages are now significantly more aware of the serious implications (including

criminal sanctions) of failing to abide by their legal obligations.

Figure 2 - Breakdown of complaints by data protection issue

Figure 2 - Breakdown of complaints by data protection issueillustrates the breakdown of complaints by data protection issue. Complaints in relation to breaches of the Data Protection Acts, 1988 & 2003 have increased from 499 in 2007 (which was 48% of the overall total) to 710 in 2008 (69% of the overall total). Complaints concerning access rights accounted for 30% of complaints overall. A total of 312 such complaints were received in 2008 compared with 187 complaints about access rights in 2007. The increase reflects a much greater level of public awareness of the right of access to personal data. This is one of the key fundamental rights enshrined in data protection legislation.

Year	Complaints received
2000	131
2001	233
2002	189
2003	258
2004	385
2005	300
2006	658
2007	1037
2008	1031

Figure 3 - Complaints received since 2000

When a complaint is received under the Data Protection Acts, I am required by Section 10 of the Acts to investigate it and to try, in the first instance, to arrange an

amicable resolution unless it is, in the terminology of the Acts, 'frivolous or vexatious'. It is very rare for my Office to have to consider that a complaint falls into that category. However, each year I receive a number of complaints in which the data subject has another agenda. In these cases the complaint to my Office may be part of a strategy designed to embarrass or frustrate a data controller. I do not allow my Office to be used for this purpose as I must ensure that the limited resources at my disposal are focused on real and important data protection issues.

As in previous years, the vast majority of complaints concluded in 2008 were resolved amicably without the need for a formal decision under Section 10 of the Acts. In 2008 I made a total of seventeen formal decisions, four of which rejected the substance of the data subject's complaint.

As Commissioner, I do not have power to award compensation. However, if a data controller fails to observe their duty of care in respect of personal data, they are liable to be pursued for damages through the courts (under Section 7 of the Acts). My Office has no function in relation to any such proceedings.

Use of Legal Powers

In my Annual Report for 2007, for the first time, I included a list of occasions when I have had to resort to the use of my legal powers to advance an investigation. This involves serving Enforcement Notices or Information Notices. Details of Enforcement Notices and Information Notices served by me in 2008 are set out in the following tables. I hope that publication of these lists will encourage all organisations that are the subject of complaints to co-operate fully with my Office in relation to our statutory investigations. While I may issue an Enforcement Notice in relation to any aspect of the Data Protection Acts, it is not normally necessary to do so. The vast majority of organisations engage with my Office and amend errant practices without the need for a formal legal notice. The Enforcement Notices outlined below all relate to data controllers that refused to provide personal data sought under Section 4 of the Acts. I view the right to access and control your personal information as one of the most fundamental rights provided by the Data Protection Acts. I do not hesitate, when necessary, to use my legal powers to ensure that data controllers comply with their obligations in this area.

Table 1 - Enforcement Notices* issued in 2008

Data Controller:	In relation to:
Able Security Limited	Section 4 (1) of the Data Protection Acts
Palatine Transport (Ireland) Limited	Section 4 (1) of the Data Protection Acts
McDermott O'Farrell Limited	Section 4 (1) of the Data Protection Acts
McDermott O'Farrell Limited	Section 4 (1) of the Data Protection Acts
McDermott O'Farrell Limited	Section 4 (1) of the Data Protection Acts
McDermott O'Farrell Limited	Section 4 (1) of the Data Protection Acts
McDermott O'Farrell Limited	Section 4 (1) of the Data Protection Acts
Broadford International Limited	Section 4 (1) of the Data Protection Acts
Total Fitness Ireland	Section 4 (1) of the Data Protection Acts

* Under section 10 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require a data controller or data processor to take whatever steps the Commissioner considers appropriate to comply with the terms of the Acts.

Table 2 - Selected Information Notices* issued in 2008

Data Controller:
St. Mary's Touraneena National School
Money Corp Limited

* Under section 12 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require a person to provide him with whatever information the Commissioner needs to carry out his functions, such as to pursue an investigation.

S.I. No. 526 of 2008

Statutory Instrument No. 526 of 2008 – the European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) (Amendment) Regulations 2008 - brought forward by the Minister for Communications, Energy and Natural Resources came into operation on 13 December, 2008. This statutory instrument amends S.I. No. 535 of 2003 which has been in operation since November 2003.

Amongst the changes in the new Statutory Instrument are:

- An increase from €3,000 to €5,000 in the penalty for a summary offence in respect of a contravention of the regulation relating to unsolicited communications;

- The creation of an indictable offence for a contravention of the regulation relating to unsolicited communications. Where the person tried is a body corporate the fine imposed may not exceed €250,000 or, if 10% of the turnover of the person is greater than that amount, an amount equal to that percentage. Where the person tried is a natural person, the fine imposed may not exceed €50,000;
- Provision is made for the prosecution of an officer of a body corporate for an offence under the regulations whether or not the body corporate itself has been proceeded against or has been convicted of the offence;
- In court proceedings for offences concerning the contravention of the regulation relating to unsolicited communications, the onus of establishing that a subscriber consented to receive an unsolicited communication will lie on the defendant.

These Regulations are a significant step in the fight against unsolicited communications for direct marketing purposes. I welcome the increase in penalties. I am confident that the strengthening of the law in this area will help me further to deal effectively with unsolicited communications, particularly unsolicited text messages. The new regulations send a strong message to all involved in direct marketing that they must comply with the law. The regulations demonstrate the Government's commitment to the role of my Office in preventing these unacceptable intrusions into our privacy.

The full texts of S.I. No. 526 of 2008 (http://www.dataprotection.ie/documents/legal/SI_526_of_2008.pdf) and S.I. No. 535 of 2003 (http://www.dataprotection.ie/viewdoc.asp?DocID=799&ad=1) are available on my Office's website.

Iarnród Éireann prosecuted for not responding to an Information Notice

In August 2007, I received a complaint under the Data Protection Acts against Iarnród Éireann (Irish Rail). My Office commenced an investigation of the complaint but, despite two letters and six telephone calls, we did not receive any response or acknowledgement. As a consequence of the failure of the company to respond to

correspondence issued as part of a statutory investigation, I served an Information Notice on Iarnród Éireann at the end of November 2007. An Information Notice is a legal notice under Section 12 of the Data Protection Acts that obliges the person on whom it is served to hand over information that I require for the performance of my functions. Unless an appeal of the Information Notice is lodged with the Circuit Court, the recipient must respond within twenty one days. A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an Information Notice shall be guilty of an offence.

In this case, Iarnród Éireann did not lodge an appeal of the Information Notice, it did not provide the information sought in the Notice and it did not acknowledge receipt of the Notice. At the beginning of February 2008 I instructed my solicitors to serve a summons on the company for an offence under Section 12(5) of the Acts. This is not my preferred approach but I had no option, since my Office still had not received any response from Iarnród Éireann.

The matter came before the Dublin Metropolitan District Court on 10 June, 2008. Iarnród Éireann was convicted of the offence.

This was the first time that the Office of the Data Protection Commissioner had to bring a prosecution against any entity for failing to respond to an Information Notice. It was particularly disappointing that a State company failed to engage seriously with a formal statutory investigation by my Office. As this case demonstrates, while I wish to use my legal powers to obtain information sparingly, I am prepared to use them when necessary. . I am also glad to say that, where subsequent issues have arisen that have required contact between my Office and Iarnród Éireann, we have received full co-operation.

Clarion Marketing Limited prosecuted for sending unsolicited text messages

During August 2007 my Office received a number of complaints from members of the public about the receipt of unsolicited text messages on their mobile phones. Some individuals complained of receiving two unsolicited text messages within the space of

a few days. My Office immediately commenced an investigation to determine the source of the text messages. We quickly established that Clarion Marketing Limited, with a head office address in the Isle of Man, was responsible for the messages. It had used the technical infrastructure of two Dublin-based companies to transmit the messages to Irish mobile phones. We also discovered that key personnel of Clarion Marketing Limited were based in Dublin and that it was through the Dublin base that the messages had effectively been sent. Over 100,000 such messages were sent to Irish mobile phones using numbers sourced from an external database purchased by Clarion.

Our investigation included an inspection of the premises used in Dublin to send the messages and contacts with the UK-based suppliers of the data and with Experian Ireland (which acted as a broker for the database). As I was not satisfied that the complainants had opted-in to receive these messages, I decided to prosecute Clarion. I instructed my solicitors to serve summonses in respect of offences committed under Regulation 13(1)(b) of SI 535 of 2003.

The case was heard on 17 November, 2008 and following extensive interactions between my Office and Clarion, Clarion Marketing Limited entered guilty pleas in respect of six charges - one each in respect of an unsolicited text message sent to the six individuals who had complained to my Office. The Court imposed a fine of €2,000.

I was very satisfied with the outcome of this case. It demonstrates that I will not hesitate to use my prosecutorial powers where I deem it necessary. I want to thank the individual complainants for bringing the matter to the attention of my Office and for indicating their willingness to give witness evidence in court. Thankfully this was not necessary after the company entered guilty pleas. It is important that the public continue to bring such marketing text message campaigns to our attention so that we can investigate their lawfulness and, if necessary, take steps to stop them.

An important feature of these prosecutions was the pivotal role played by my colleague the Data Protection Supervisor in the Isle of Man. Throughout our investigation we maintained close contact with him and the information which he

provided was crucial in bringing successful prosecutions. I wish to thank him formally for the time and effort given by him and his Office. This is an excellent example of how regulatory authorities can work effectively together, even across national boundaries.

These prosecutions were a part of a series of prosecutions in relation to unsolicited direct marketing text messages by my Office. I commented on my determination to deal with this issue in last year's report. Another batch of 350 prosecutions remain before the Courts as they were subject to a High Court Injunction granted to Realm Communications. The substance of the injunction was heard in the Commercial High Court on 15/16 July 2008. I am pleased that the judgment which was delivered in the early part of this year rejected the challenge and awarded costs to my Office.

Circuit Court allows appeal of an Enforcement Notice

In November 2008 the Dublin Circuit Court allowed an appeal of an Enforcement Notice which I had served. The background to the case was that a data subject had sought deletion of their records by a data controller under Section 6A of the Acts on the basis that the processing of their personal data by the entity was causing damage and distress and that this damage and distress was unwarranted. Following an extensive investigation I concluded that the data subject's case was justified and served an Enforcement Notice as provided for in Section 6A(5) of the Acts requiring the entity to comply in full with the data subject's request. This was appealed under Section 26 of the Acts. The Court disagreed with my assessment, revoked the Enforcement Notice and allowed the appeal.

Complaints regarding Chorus and NTL

During 2008 my Office handled almost thirty complaints made by individuals against Chorus and NTL which have merged to become one company, UPC. The complaints covered a range of data protection issues but focused in particular on direct marketing issues. This volume of complaints against one company is significant. However, I understand that UPC is a large user of personal data and conducts targeted marketing campaigns which, by their nature, can lead to complaints. My Office had received complaints in lesser numbers about this company in previous years but towards the end of 2007 the volume began to increase significantly.

In the direct marketing category, complaints were submitted in respect of postal, telephone and text message marketing by UPC. As a result of the increased volume of complaints, I instructed my staff to conduct an inspection of UPC under Section 10(1A) of the Acts to ascertain if the procedures and practices employed by UPC were in compliance with the provisions of the Acts. This broad-based inspection took place in May 2008. Afterwards, in accordance with normal practice, my Office issued a number of recommendations to the company as part of an audit report.

In regard to the complaints handled by my Office in 2008, those which were upheld were all resolved amicably. In addition, the company carried out a number of improvements to its systems and procedures which had the effect of significantly reducing the number of complaints submitted to my Office. While I welcome the steps taken by the company to increase its level of data protection compliance during 2008, there is no room for complacency. I will pay close attention to any complaints received against this company in the future to ensure that there is no slippage in terms of compliance.

I am grateful to each individual who lodged complaints with my Office about UPC. They brought to my attention a range of data protection issues that needed to be addressed by the company. I am confident that my Office's efforts to resolve those complaints will yield benefits for the data protection rights of all customers, ex-customers and, indeed, non-customers of UPC.

Privacy Audits

I am empowered to carry out privacy audits and inspections to ensure compliance with the Acts and to identify possible breaches. Scheduled audits are intended to assist the data controller in ensuring that their data protection systems are effective and comprehensive. These audits are in addition to investigations carried out by my Office in response to specific complaints. My Office also continued with unscheduled inspections under powers conferred under section 24 of the Data Protection Acts in response to specific issues of concern.

Department of Social & Family Affairs

A number of allegations of inappropriate access to information held by the public sector, together with specific information concerning the Department of Social and Family Affairs obtained by my Office in the course of audits of insurance companies, led to an intensive audit of that Department by my Office in 2008. My principal concern arose in relation to allegations that data held by the Department of Social & Family Affairs was made available to private investigators engaged by insurance companies. Upon conclusion of my investigation into this matter, I was satisfied that there was sufficient evidence to indicate that private investigators were granted unlawful access to personal data held by the Department of Social & Family Affairs.

On this basis my Office conducted an intensive audit of the Department of Social & Family Affairs in the early part of 2008. The resulting report contained a series of recommendations concerning access management, security, data sharing and data protection policies. The Department of Social & Family Affairs published the audit report in full on its website:

Report of the Data Protection Commissioner on Data Protection in the Department of Social & Family Affairs (http://www.welfare.ie/EN/Topics/Documents/ODPCReport.pdf)

I am pleased to note that the Department has responded to the recommendations contained in the report. The Department of Social and Family Affairs issued a progress report to my Office in December 2008. The update demonstrates the considerable efforts of the Department to put in place procedures reflecting a strong commitment to improving data protection standards. In particular, the measures taken by the Department to control all external access and transfers to and from its systems are to be commended. I also welcome the Department's roll-out of meaningful data protection training for its staff. This is a challenging process in an organisation as large and complex as the Department of Social & Family Affairs. Of course, there is still work remaining for the Department. Nonetheless, I am satisfied that it takes its responsibilities in relation to customer data seriously and has procedures in place to assist in meeting these responsibilities.

In 2008, I also commenced an audit of the Revenue Commissioners, another public sector entity holding substantial amounts of personal data. The initial stages of the 2008 Revenue audit programme were focused on obtaining an overview of the organisation in terms of the capture and movement of personal data within it. This initial exploratory stage allowed the audit team to identify priority areas, systems and processes for inspection. A further series of audits of Revenue are scheduled to take place throughout 2009 in various locations across the country. I will report on this in next year's Annual Report.

In the course of 2008, 28 audits were carried out by my Office. This is a substantial increase on the previous year in which 12 audits were completed. I intend to pursue this ambitious audit programme in 2009.

The rationale behind the selection of target organisations for audit is to reach a broad mix of public, private and voluntary sector entities holding personal data. Audit targets may be selected, for instance, on foot of complaints received by my Office or on foot of specific allegations in media reports. However, many organisations are selected for audit purely because they are representative of a particular sector. In most cases it is my hope that the conduct of an audit in a particular sector will have a multiplier effect across a sector and serve to raise standards generally.

Organisations audited in 2008:

Department of Social & Family Affairs

Pure H20

MBNA

UPC Communications

Dunnes Stores

Sligo Social Welfare Office

St James' Hospital

An Post

Data Ireland

Veolia Transport Ireland

Holy Family Secondary School, Newbridge

Wyeth Pharmaceuticals

Trócaire
Dublin Institute of Technology
Gallic Distributors (Citroen)
Drogheda Community CCTV Scheme
Soho Bar, Cork
Thom's Publications Ltd.
Bill Moss Partnership
South Dublin County Council
The Revenue Commissioners
National Vehicle Drivers File (NVDF), Shannon
Ryanair
D-Doc, North Dublin's GP Out of Hours Service
Sheraton Hotel, Athlone
Laois Motor Tax Office
Finglas Child & Adolescent Centre
White Sands Hotel, Portmarnock

As in previous years, my inspection teams found that there is a reasonably good awareness of, and compliance with, data protection principles in the organisations that were inspected. I am pleased to report that, in response to our suggestions, the data controllers appeared willing to put procedures in place to ensure that they met their data protection responsibilities in full. This is very heartening as it indicates that organisations of all sizes are beginning to realise that good data protection practices are important to customers. I would like to thank all of the organisations audited and inspected throughout the year for their cooperation.

Data Breach Notification

The Data Protection Acts oblige all data controllers to adopt 'appropriate' security measures to safeguard personal data that has been entrusted to them. In deciding what constitutes appropriate security measures, data controllers must take into account the harm that might result from unauthorised processing or accidental loss of the personal data that they hold. They must also take into account the nature of the data concerned. The cost of implementing security measures and the availability of

appropriate technology may also be taken into account. The data controller must take reasonable steps to ensure that employees comply with the security measures in place.

The Electronic Privacy Regulations impose more specific obligations on telecommunications providers – including an obligation to inform subscribers of any particular risk of a breach of security (Regulation 4(2) SI 535 of 2003 - http://www.dataprotection.ie/viewdoc.asp?DocID=799&ad=1).

Over the past year my Office has been intensifying its efforts to encourage public and private sector bodies to voluntarily report personal data security breaches to the Office. This approach has met with considerable success and breach reporting has come to be commonly viewed as part of best practice when confronted with such incidents. Since August 2007, 86 breaches have been reported to the Office by 57 different organisations (see Figure 4 - Number of data security breach reportsbelow). In any case, given the national and international focus on this issue, the Minister for Justice, Equality & Law Reform took the initiative to establish a High Level Group on Data Breach Notification to advise him on whether the mandatory reporting of breach incidents in certain situations should be introduced. I am a member of this Group and look forward to its report later in 2009 and any necessary follow-up by way of legislation and oversight by my Office.

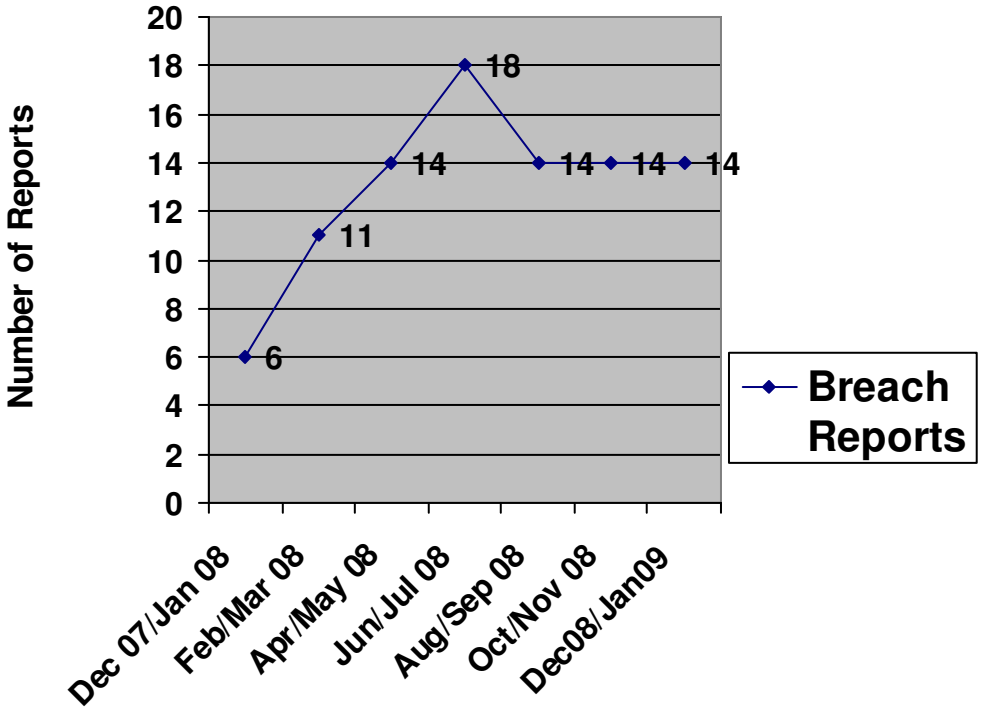

Figure 4 - Number of data security breach reports

As Figure 4 - Number of data security breach reports indicates, levels of awareness and reporting practices have improved significantly since early 2008. Awareness seems to be reasonably high in both the private and public sectors; 36 of the organisations reporting data security breaches in 2008 were private sector organisations and 21 were from the public sector. This may reflect the impact of high profile breach cases involving organisations from both sectors in Ireland and in neighbouring jurisdictions. About half of the organisations that reported breaches could be classified as large organisations (100 staff or more). Breaches reported by these organisations most commonly related to failures to properly protect data on laptops or other devices, errors in automatic mailing systems, insufficient staff access controls and inadequate direct marketing controls. Among smaller organisations the causes of breaches are more diverse. Common reports among smaller organisations include failure to properly protect data on laptops or other devices and loss of hard copy data. As might be expected, breaches involving small organisations tend to

affect smaller numbers of data subjects though the nature of the data lost can be as serious as any lost by larger organisations.

As mentioned above, certain data security breaches attracted a considerable amount of attention among members of the public concerned at the implications of the cases for their personal privacy.

Jobs.ie

In March I launched an investigation in relation to the illegal access and download of CVs by persons unknown on the website of Jobs.ie, an online recruitment company. The investigation was helped by a high level of cooperation from the company and found that parts of the company's web systems were not appropriately secured. We also found that the company sometimes held on to personal information for an unnecessarily long period of time, without the consent of the individuals concerned. The company moved quickly to secure its systems and I commended it for the manner in which it responded to the breach.

Bank of Ireland

In April I launched an investigation in relation to a series of thefts and losses of Bank of Ireland Life laptops which had taken place between June and September 2007. The focus of the investigation was to determine:

- the exact nature of the personal data on the laptops;
- how and why that data came to be on the laptops in the first place; and
- what specific security was in place to protect the personal data while on the laptops.

I was satisfied at the conclusion of the investigation that Bank of Ireland had a shared view of the seriousness of the incidents in question. The Bank had already put in place, or was in the process of putting in place, measures to minimise the risk of a repeat of the incident. In fact such a security upgrade was already underway prior to these incidents.

The laptops stolen were used by employees of Bank of Ireland Life in the course of their duties. Information was held on the laptops from 3 distinct databases containing

customer information. My Office was satisfied that the information supplied by Bank of Ireland to its customers about the data downloaded to the laptops was a true and accurate reflection of all the data residing in the databases. This matter was examined closely by my Office.

Bank of Ireland Life indicated that the use of laptops by its staff in the course of their duties is part of the modus operandi of the industry. Staff members have to be very mobile, needing to travel to locations of the customer's choice. They need to be in a position to respond to customer requirements immediately and without prior notice. In those circumstances, Bank of Ireland considers that its staff members need to have a large amount of customer information available to them.

The stolen laptops had what the bank termed as 'three-level' password protection. Bank of Ireland investigated the matter and came to the view that the password protection was not sufficiently secure.

Bank of Ireland customers were not informed of the disclosure of their data until between six and eights months after the original disclosure. This appears to have resulted from an error in the Bank's business processes. These processes required that laptop thefts should be reported to sales managers (and to An Garda Síochána) but they were not sufficiently robust to ensure that the thefts were reported by sales managers to senior management.

In regard to the delay in Bank of Ireland becoming aware of the loss of the laptops, the Bank indicated that the issue only came to light in mid-February 2008 when information was sought from all business units about missing laptops. There was a subsequent additional delay in reporting the matter to this Office. It is understood that this delay resulted from internal investigations and the time it took to establish that there was a legitimate concern in relation to the level of security in place on the laptops. I accepted that Bank of Ireland required some time to complete its initial investigation and to assess ongoing risks to customers but I would have preferred to have been notified earlier. It should be pointed out, however, that there is no express requirement under the Data Protection Acts for Bank of Ireland to have informed either customers or this Office of the loss of the personal data in question.

The Data Protection Acts require that appropriate security measures be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of personal data. In view of the storage of the laptops and the lack of security measures appropriate to the large volume of personal data contained on the laptops, I concluded that Bank of Ireland Life failed to meet this requirement by not having in place appropriate security measures.

I received a number of complaints from people affected by this incident. However I am glad to say that it was possible to reach an amicable resolution in all of these complaints. Bank of Ireland Life made a sizeable charitable donation in respect of all the customers affected. Equally, Bank of Ireland had also given a commitment that no customer would suffer any financial loss arising from the incident. I was satisfied with this outcome.

Office of the Comptroller and Auditor General

In July I was notified by the Office of the Comptroller and Auditor General (C&AG) that three of their laptops containing personal data had been stolen over recent years. The personal data was collected in the course of audits of a number of organisations conducted by the C&AG. One of the laptops contained 379,514 social welfare records. My Office's investigation examined:

- the security profile of the C&AG's information management systems;
- the nature and amount of data lost; and
- the office's data retention, access and security policies.

I also considered the apparent delay in reporting the thefts to my Office. From the outset of the investigation the C&AG adopted an open and cooperative attitude that was helpful in completing the investigation. My investigation found that the C&AG did not have appropriate security controls in place on the stolen laptops. A failure in their internal reporting systems accounted for the greater part of the delay in informing me, though I would have preferred to have been informed earlier after the thefts came to light. However, I recognise the measures already taken by the C&AG to address the issues raised by these incidents. These measures included full disk

encryption of all C&AG laptops and other portable memory devices, guidance and training for staff and the roll-out of comprehensive security incident procedures.

I wish to again welcome the manner in which the Department of Social & Family Affairs (which was blameless in relation to the loss of the data) sought to address the issue by contacting all of those directly affected by the incident. The Department also put in place a dedicated helpdesk to provide further information as required to those who were affected. This represented best practice and was a truly first rate response in the circumstances. There is no doubt that it served to minimise the concern felt by those persons whose data was lost.

Health Service Executive (HSE)

In September I launched an investigation in relation to the theft of a HSE laptop containing the personal information of certain HSE staff. As a result of delays in obtaining explanations relating to the basis for collecting the information that was stored on the laptop, this investigation was still ongoing at the end of 2008 (it has since been concluded). Following a number of data breach incidents involving personal data held by the HSE, senior officials from my Office met with senior management in the HSE to discuss a number of concerns regarding data security. I have outlined below a number of my general concerns in relation to the processing of personal data under the control of the HSE.

Department of Finance Guidance on Data Protection

During the course of 2008, the Department of Finance worked on producing an extensive guidance note entitled "Protecting the confidentiality of personal data." The note is available on the Department of Finance website and can be accessed at: http://www.ict.gov.ie/docs/Data Protection guidelines - final.pdf

The guidelines aim to assist Government departments, offices and agencies "in implementing systems and procedures that will ensure, as much as possible, that personal data in their possession is kept safe and secure and to help departments, offices and agencies meet their legal responsibilities." The guidance note encourages Government bodies to put in place data security breach management plans to follow in the event of a breach incident. Acknowledging that there is no explicit legal obligation to notify those affected or other bodies in the event of a data security

breach, the draft guidance note states that breach incidents should be reported immediately "both internally and to the Data Protection Commissioner's Office and, if appropriate in the circumstances, to the persons whose data it is."

Data Protection Code of Practice for the insurance sector

In August, I approved and published a Data Protection Code of Practice for the Insurance Sector under Section 13 of the Data Protection Acts. The Code was prepared against a backdrop of significant public concern arising from media reports which emerged in 2006. These reports claimed that personal information held by An Garda Síochána and by the Department of Social & Family Affairs was being routinely accessed by private investigators acting on behalf of insurance companies. The claims were confirmed during subsequent investigations of insurance companies by my Office. The Code is an important element of my Office's response to those issues.

While the Code was the subject of extensive discussion with the Irish Insurance Federation (IIF) and individual insurance companies, it did not, unfortunately, prove possible for the IIF to agree to all of the terms of the Code on behalf of its members. However, I firmly believe that the approved Code provides a clear framework for insurance companies to process their customer data in accordance with the Data Protection Acts. It will also act as an assessment tool for the examination of any complaints received by my Office in relation to the handling of personal data within the insurance sector.

The Data Protection Acts provide for the preparation of sector-specific codes of practice that facilitate a better understanding of the requirements of the Acts as they apply to a particular sector. This Code clarifies how data protection rules apply specifically in the insurance sector, making it simpler for the sector to meet its obligations in relation to the processing of personal information. The insurance sector holds extensive personal data, some of it extremely sensitive, on a large part of the population. I hope and expect that the publication of the Code will result in improvements in data protection compliance in the insurance sector. Such improvements will benefit both the sector and the consumer. Since it was published in August, I am happy to say that my Office has received regular queries from

insurance companies regarding the Code and how it applies to their organisation. I am encouraged that the provisions of the Code are actually being implemented to the benefit of the sector and consumers alike.

I also expect that the Code will help consumers to understand how their personal data is used in the insurance sector and what standards they should expect in this regard.

I should also mention that An Garda Síochána carried out an extensive investigation in relation to the allegations that personal data held by it were being accessed and made available to insurance companies.

Promoting awareness

Educating individuals about their rights under the Data Protection Acts and ensuring that organisations are aware of their responsibilities continues to be a key focus for my Office.

To measure levels of awareness of data protection rights and to explore the particular privacy issues that concern members of the public, my Office commissioned a public awareness survey in April 2008. This was a follow-up to similar surveys conducted in 2002 and 2005. I also continued to pursue an awareness campaign targeted at young people. A new training initiative (a 'Data Protection Road Show' held in Sligo in March 2008) was targeted at data controllers in the North-West region. Another new awareness-raising initiative, a video clip competition entitled 'Privacy in the 21st Century', was organised by my Office in 2008 in association with YouTube/Google.

Each year my Office receives a large number of requests for data protection training from organisations operating within the public, private and voluntary sectors. While the Office is not in a position to offer formal training as such, we seek to assist organisations within these sectors by giving presentations at appropriate events. During 2008, the Office made 61 presentations in total, an increase on the number of presentations given in 2007.

Public Awareness Survey 2008

The results from the 2008 survey indicate many individuals continue to be very concerned about the privacy of their personal information. Some of the key findings from the survey are as follows:

- Nearly two thirds of the population believe that they have personally experienced an invasion of privacy at some level.
- 67% of people who use the internet regularly are concerned about the amount of information requested when signing up or registering on a website.
- 63% expressed concern about internet logs being retained and monitored.
- Almost 1 in 4 Dublin respondents stated they had "information, images or footage" of themselves posted on the internet without their consent in comparison with an overall national figure of 11%.
- Unsolicited direct marketing, regardless of the type of medium used, continues to cause concern. The survey findings indicate that discontent with unsolicited text and email marketing has significantly increased since 2005.

The findings from the 2008 survey indicate lower levels of awareness amongst the unemployed, self-employed and respondents who do not use the internet. Similarly to the 2005 awareness survey, the age groups displaying lower levels of awareness are the upper and lower age groups (65+ and 15-24 year olds). Respondents in the 35-49 age category display the highest levels of awareness. In so far as our resources permit, my Office will continue to strengthen our engagements with information service providers whose client base includes the unemployed, self-employed and elderly to heighten awareness of the rights and obligations under the Data Protection Acts 1988 & 2003.

Survey Key Findings (http://www.dataprotection.ie/documents/trainingandawarenes/PAS08.pdf)

Survey Full Report (http://www.dataprotection.ie/documents/press/Survey08.pdf)

12-18 year olds awareness campaign

As indicated above, awareness of data protection rights among younger people continues to be rather low. As a result, I have continued to develop awareness campaigns targeted at the 12-18 year old age group.

This awareness programme featured the publication of a new data protection resource aimed at second level schools - *Sign Up, Log In, Opt Out: Protecting Your Privacy & Controlling Your Data* (*http://www.dataprotection.ie/docs/CSPE_Booklet/862.htm*) . The then Minister for Education & Science, Mary Hanafin TD, officially launched this resource on Data Protection Day (28th January 2008). The resource was distributed to all secondary schools nationwide. Presentations on the resource were provided at a series of in-service CSPE teacher training days in 2008.

As part of the awareness drive aimed at young people, my Office had a stand at the Young Social Innovators exhibition in the RDS, Dublin in May 2008. As well as promoting awareness of data protection and privacy matters affecting young people, we took the opportunity to survey young people attending the event to measure levels of awareness of data protection issues and the extent to which young people are concerned with protecting their information.

YSI Survey Key Findings
(http://www.dataprotection.ie/documents/teens/YSI_2008_-_key_findings.pdf)
Full Survey Report
(http://www.dataprotection.ie/documents/teens/YSI_2008_-_Survey_-_Full_Report.pdf)

Video clip competition

An innovative video clip competition was also launched on 28 January 2008 by the then Minister for Education and Science, Mary Hanafin TD. The competition sought short video clips on the theme of 'Privacy in the 21st Century' and was organised by my Office in association with YouTube. The competition had a total prize fund of €10,000 and attracted a high standard of entries that provided a creative and entertaining look at a range of privacy issues.

The winning clips are available to view at:

First prize http://ie.youtube.com/watch?v=UOpIzHJgZ4o

Second prize http://ie.youtube.com/watch?v=LeMfkGkuFvs

Third prize http://ie.youtube.com/watch?v=TC8W_tBXQnE

Gallery of entries to the competition http://www.youtube.ie/dataprotection

Training opportunities

A core focus of this Office is to promote awareness among organisations of their responsibilities when processing personal information.

During the year, my Office devised a new training initiative in the form of a 'Data Protection Road Show' delivered by staff from my Office. The Road Show was targeted at data controllers and processors in a particular region of the country. In this regard, the Office held a seminar for data controllers and data processors based in the North West area in Sligo on March 13, 2008. The seminar provided a valuable opportunity for organisations in counties Sligo, Mayo, Leitrim, Donegal and Roscommon to develop their data protection knowledge. I intend to organise similar events in the future when resources permit.

The following training aids and guidance material are available free of charge to assist organisations in raising staff awareness of their responsibilities when processing personal information:

1. Booklet - A guide for data controllers
http://www.dataprotection.ie/docs/A_Guide_for_Data_Contollers/696.htm

2. Booklet - A guide to your rights
http://www.dataprotection.ie/docs/A_Guide_to_Your_Rights/699.htm

3. Training DVD - 'My Data, Your Business'
http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/video/video2.htm&CatID=69&m=p

Facilitator's Guide to DVD

http://www.dataprotection.ie/docs/Facilitators_Guide/283.htm

4. PowerPoint Presentations
http://www.dataprotection.ie/docs/Generic_Presentations/439.htm

5. Rights & Responsibilities Chart
http://www.dataprotection.ie/docs/Chart_'Rights_&_Responsibilities'/703.htm

Hardcopies of the booklets, chart, DVD and Facilitator's Guide can be obtained by contacting my Office.

National and Regional Policy Issues

Personal Public Service Number (PPSN)

My 2007 Report highlighted the extended use of the PPSN as one of the "Top Ten Threats to Privacy". I have availed of the opportunity to flag the phenomenon of function and information creep a number of times in the past few years. 2008 has, if anything, seen a further expansion in use of the PPSN without full consideration of the potential consequences.

I fully acknowledge that the PPSN can have an important role to play in the efficient delivery of certain public services – efficiency being an increasingly important consideration in times of budgetary constraints. But I am increasingly concerned at a tendency to seek the PPSN where there is little justification for its use. Of even greater concern is a tendency to extend its use into the private sector. Such indiscriminate use of the PPSN carries clear dangers both in terms of irregular sharing of personal data between organisations and as a facilitator of identity theft.

I am concerned that the PPSN, entirely without debate and reasonable consideration, is becoming the stock answer to facilitating data collection, analysis and exchange. It is seen by some as the solution to all barriers to information sharing. I find it hard to be convinced by such arguments even at a practical level and I am convinced, in light of experience elsewhere, that over-reliance on one form of identity creates weaknesses in security. Such over-reliance undermines privacy but also

exponentially increases the potential for identity theft. It is only necessary to review the well-documented deficiencies which have emerged in relation to the US Social Security Number (SSN) which the US authorities are working very hard to resolve. Problems associated with the SSN have resulted in high rates of identity theft and other privacy and confidentiality issues. Thankfully I am not alone in my stance on this issue and Government policy at present is that the use of the PPSN must remain narrow. However, this is often not well understood on the ground. In this respect, I am very supportive of ongoing work which the Department of Finance (via its technology division CMOD) is undertaking in relation to issues of identity management. They are working to enable public services to more easily identify their customers based on information already held and without relying on the PPSN. I have liaised closely with CMOD on this work and will continue to do so. The project seeks to take on board legitimate privacy concerns while at the same time supporting the public service in the delivery of efficient and effective services.

The use of the PPSN is governed by the provisions of the Social Welfare Miscellaneous Provisions Act 2005. It can only be requested by specified bodies where the transaction relates to a public function of that body. However, the concept of 'public function' is constantly expanding, especially in relation to the legitimate collection of the PPSN by private commercial entities as a result of their reporting obligations to Public Bodies. I outline an example of this later in relation to my Office's engagement with the Revenue Commissioners and the banking sector. I am particularly concerned when we discover legislative provisions expanding the use of the PPSN without due consideration of the privacy repercussions. It is revealing that the Department of Social & Family Affairs (which has responsibility for issuing the PPSN) does not consider the PPSN to be sufficiently robust from an accuracy and verification perspective to be relied upon as a unique identifier. In the context of the consistent views of the Department of Finance, the Department of Social & Family Affairs and my Office on this issue, it is surprising that demands for the expansion of the PPSN continue and ever more entities seek to use it.

Aside from direct service provision, extensive use is made of the PPSN for other purposes. These can include the production of statistical information and, in certain cases, for eligibility verification where exchange of data between Government

Departments and Bodies is deemed necessary. It is important that such data exchange has a clear justification; that, in general, the individuals involved are fully aware of it; and that there is a basis in law for the exchange either under the Data Protection Acts or specific legislation.

As a potential unique identifier, there is a trend towards using the PPSN as an added security verification feature for computer systems. My Office has dealt with queries regarding both public and private sector organisations who are seeking to use the PPSN for this purpose. Any use of the PPSN as a log-in or password is not permissible and I have sought to bring such practices to an end. In an employment context, there is a strict statutory basis providing for the use of the PPSN Any other use made of the PPSN is unlikely to be in conformity with the provisions of the Social Welfare Acts or the Data Protection Acts. We have also encountered organisations which are not on the register of PPSN users (the register can be viewed at http://www.welfare.ie/EN/Topics/PPSN/Pages/rou.aspx) but which have included a field in their systems for requesting and storing the PPSN. They do this on the basis that they may be obliged to collect the number at some future point. In these cases the field was active and the PPSN was being inputted by staff that were unaware of restrictions regarding the use of the PPSN. This is clearly not acceptable and in response my Office ordered the deletion of any data collected and the removal of the field.

I am aware of the proliferation of uses for the PPSN in the health sector through our engagements with that sector. The issue of a universal health identifier is being considered by the relevant agencies and this is a matter which is discussed in more detail in the section below dealing with the proposed Health Information Bill.

Our close monitoring of this issue will continue and we will continue to develop awareness that the PPSN must be collected and used within strict legislative boundaries.

Financial Institutions' requirement to seek the PPSN

Financial institutions are required to seek and retain PPSNs of persons opening certain interest-bearing accounts after 1 January 2009. The Revenue Commissioners consulted my Office on this matter prior to the making of the relevant Regulations by the Minister for Finance. I thank the Office of the Revenue Commissioners for approaching my Office in such an open, constructive and transparent manner on this issue. The financial institutions were required to retain the data on computer systems and then to provide the data to the Revenue Commissioners.

As current accounts now also carry significant amounts of interest, this provision, in practice, requires financial institutions to seek and hold PPSNs in relation to all new account holders. I had significant concerns about the privacy implications of the proposals.

Helpfully, the Revenue Commissioners recognise that the PPSN is a valuable piece of personal information that must be safeguarded against misuse. In this context, my Office sought strong justification for any extension of its use.

My Office has a long-standing position in relation to the collection of PPSNs by financial institutions under anti-money laundering requirements for interest bearing accounts. Documentation containing the PPSN should be seen, copied and put on a file for future review by the Revenue Commissioners or other supervisory bodies, including auditors. However, the actual number should not be recorded separately. This purpose limitation for the use of the PPSN has been well understood and implemented.

By requiring the electronic retention of PPSNs, the new regulations go significantly beyond this framework and create the possibility of matching accounts of individuals across different platforms and branches based on a single identifier. Clearly, this was a major concern from a privacy perspective. The PPSN could also potentially be used to facilitate the sharing of information between financial institutions about a person's

profile. It is important to note that representatives of the financial sector made absolutely clear that they had no wish to do this.

From a data security perspective, including PPSN information at customer account level creates additional risks of inappropriate access to information. It also risks creating a reliance among financial institutions on using the PPSN as a means of identifying customers. It is my firm view, as I have indicated above, that the lack of a single identifier has been a key element in ensuring that Ireland, thus far, has not suffered the same degree of problems in regard to identity theft as other jurisdictions.

For these reasons, as a prerequisite for the proposals to proceed, I sought the insertion of appropriate privacy safeguards. As a result, the Regulations state that it is an offence for any financial institution to use the PPSN collected on behalf of the Revenue Commissioners for any purpose other than those stipulated in the regulations. We also sought amendments to the regulations to ensure that the PPSN should only be stored for a defined period and in a particular manner.

The Revenue Commissioners also undertook to work with my Office to develop guidelines to assist financial institutions in implementing the Regulations (Return of Payments Regulations 2008 (S.I. No. 136 of 2008)). The guidelines are available at: http://www.revenue.ie/en/practitioner/law/notes/guidance-note-interest-reporting.pdf
The guidelines clarify that:

- The PPSN may only be used for the purpose of reporting to Revenue under the new Regulations;
- Any other use of the PPSN can attract a penalty;
- While the PPSN may be stored at customer level, it should not be possible to search using the PPSN as the search criteria or part of the search criteria:
- The PPSN should not be shown as part of the customer's standard data: and
- The documentation that can be sought to verify the PPSN is explicitly listed.

I view our engagement with the Revenue Commissioners on this issue as an example of dialogue and co-operation leading to a policy initiative with appropriate privacy safeguards built-in.

M50 Barrier-Free Tolling Project

The operation of the M50 Barrier-Free Tolling Project generated a large number of queries to my Office last year. While the project had the clear objective of improving traffic flows on the M50, the previous model of paying cash at toll booths was at least privacy-friendly, if not the most traffic-friendly option! The National Roads Authority (NRA) first approached my Office to discuss the data protection issues associated with the operation of such a scheme in October 2007. We have engaged with them since then about this project. While I recognised that the project was challenging from a number of perspectives (not just privacy), I had concerns about the extent of the processing of personal data envisaged.

At the outset we were satisfied that an appropriate legal basis existed for permitting the processing of large amounts of personal data by a private operator who must be given access to official vehicle records to collect tolls on behalf of the NRA. Our discussions then focused on the need for a clear and agreed policy on retention periods for personal data, as required by the Data Protection Acts. We continue to recommend that retention periods should be kept to a minimum given the potential to build up a large database of information revealing details of journeys undertaken by members of the public. In the course of our engagement with the NRA, my Office also sought a privacy-friendly payment option and details of procedures regarding law enforcement access to retained data. We have reminded the organisations involved of their obligation to keep personal data safe and secure.

Overall, I have been impressed by the volume and nature of queries received from members of the public about this project. It has revealed a keen awareness of the privacy implications of barrier-free tolling. Our engagement on the operation of the scheme has been productive but has not been finalised. However, given the positive nature of our exchanges to date, I am confident of achieving an agreed approach on the remaining issues. In view of the large amount of data relating to motorists and their journeys, I will be watching the operation of the system by the NRA and its agents closely.

Limerick Regeneration Project:

My Office always prefers to be approached for views during the early stages of a project involving the collection and processing of sensitive personal information. The guidance we offered to the Limerick Regeneration Project during the year is a good example of this. Our involvement focussed on certain social regeneration objectives which were identified as priorities in the master plans for the target areas in the Limerick City region.

The following extract is taken from the Limerick Regeneration Vision Plans as published:

"The Data Protection Act is a very important and necessary piece of legislation in Ireland. However, some public servants appear to take a very rigid interpretation of this legislation. ***We do not think that the legislation was ever intended to act as a barrier to the provision of much needed and urgent services to very vulnerable people.*** *It is essential that the key state service providers urgently develop a clear and workable policy on data protection in order for information to be shared for the betterment of very vulnerable citizens. It should be possible to do this without the necessity of changing the legislation. However, if it is not possible then the legislation should be reviewed."*

I am always anxious to dispel any perceptions of data protection legislation as an insurmountable obstacle to the legitimate sharing of information. The Data Protection Acts set out a range of rights for individuals in relation to how their personal information is used but the Acts also provide for qualifications to these rights in certain circumstances. I was, therefore, very happy to be involved in providing any assistance possible in progressing this unique and challenging project. In our initial discussions we sought to demystify some of the perceptions of data protection and work through issues to find workable solutions, where necessary, in compliance with the Acts.

During our initial meeting with a large number of local agencies in February of last year, we discussed methods of enabling the sharing of information by capturing consent, by using pre-existing legal gateways or where sharing is clearly in the vital interests of an individual. We are delighted that the central agencies have taken on

board our recommendation that they should quantify the problems and issues they are encountering and develop proposals based on general advice provided by my Office. On foot of this, we held a further meeting with staff of the Regeneration Agency and the HSE to discuss a draft protocol for the sharing of family information in accordance with data protection principles. We await further updates as the project develops and we have reiterated our willingness to deal with any issues presented to us as quickly as possible.

In many ways I see this as an excellent example of a situation in which, at the outset, the Data Protection Acts were perceived as an impediment. In some respects this is understandable when dealing with the provision of necessary services to some of the most vulnerable members of society. Through extensive and constructive engagement, I believe we have facilitated all involved to more clearly establish what information they need and who is best placed to act upon that information. This more precise identification of the necessary information assists all involved by avoiding information overload and providing clarity about the best organisation to provide the necessary service. Finally, a better outcome is assured for everyone when people feel confident about providing information. They are more likely to feel confident when they have been reassured that the information will be kept confidential and will only be used to provide them with a service.

Concerns relating to the use of data relating to minors by a local authority

This issue arose following the receipt of a complaint relating to the use and retention of the personal data of a minor by a local authority in the context of its estate management functions in local authority estates.

Section 62 of the Housing Act 1966 provides that a local authority may re-possess a local authority rented dwelling for breaches of the tenant landlord tenancy agreement. Section 3 of the Housing (Miscellaneous Provisions) Act 1997 (as amended) provides that Excluding Orders may be issued by the District Court on application in relation to persons engaged in anti-social behaviour. Section 3(6) of the Housing (Miscellaneous Provisions) Act 1997 provides that such Excluding Orders expire **three** years after they are made.

I respect the obligation on local authorities to ensure good estate management in local authority estates for the benefit of everyone living there. I am satisfied that a legal basis exists for the collection and processing of personal data arising in this context. To fulfil these functions, local authorities have designated officers to investigate complaints from tenants about anti-social behaviour. It is a natural consequence of the performance of such functions that local authorities will collect personal information about the people making the complaints, the people complained about and any parties to the complaint. However, all such processing of personal data must comply with all the requirements of the Data Protection Acts.

My particular concerns related to the requirement to only use personal data for the purpose for which it was collected and that personal data should not be kept for longer than is necessary for that purpose. The Data Protection Acts require that personal data collected for one purpose or purposes may not be processed for a further purpose without a legitimate basis. This means that personal data collected as part of investigations arising from complaints received in the performance of local authority estate management functions may only be used for that or a strictly related purpose. In this and in some similar cases the data collected as part of these investigations was routinely used for further purposes such as assessing housing applications. It was not clear to my Office that a valid basis existed for such use in the Data Protection Acts other than where legally issued eviction orders or excluding orders were made. Allowing issues such as the receipt of an advisory letter or participation in a case conference (with no subsequent legal excluding order) to influence decision-making in this area is highly problematic from a data protection perspective. I am aware that Section 15 of the Housing (Miscellaneous Provisions) Act 1997 provides a basis of sorts for the use of such information for other purposes. However I was not satisfied that this legal basis or its boundaries were known or even understood in the particular complaint I had to investigate.

In addition, the Data Protection Acts provide that personal data shall not be kept longer than is necessary for the purpose for which it was obtained. In this respect, this Office has taken note of the recommendations of the National Retention Policy for Local Authority Records produced by the Local Government Management Services

Boards (LGMSB). These recommendations appear to allow for a 15 year retention period for records created in relation to anti-social behaviour. I consider that a 15 year retention period for all records created in this area (regardless of whether an excluding order was issued or an eviction was granted) is excessive. While a case can be made for holding records relating to excluding orders and evictions for this period, such a case cannot be made where the only records on file are interim administrative steps. Far shorter retention periods are required in these cases; two years might be more appropriate. If no further entries have been made on a file during that period, such records should be destroyed.

Even in the case of excluding orders, as highlighted above, it is a statutory requirement that excluding orders expire after a maximum of three years. Provision is made for them to expire after a shorter period at the discretion of the Court. Given the statutory provision limiting the period of application of an excluding order, there does not appear to be a clear legal basis for reliance upon them for estate management purposes after that period.

The passage above outlines the requirements of the Data Protection Acts as they apply to records regarding estate management functions generally. Perhaps the most important issue is that these considerations are amplified when the records held relate to minors. This is a matter of established jurisprudence domestically and in the European Court of Human Rights. Additionally, domestic legislation specifically provides for the sealing of certain criminal records and their non-disclosure when they relate to minors. On this basis, I was extremely concerned that there was no focus on establishing special measures to restrict use of any such records relating to minors. Most significantly, any such records about minors should be deleted after a very short period if the file relating to the young person is no longer active. It must be assumed that a young person can be rehabilitated and, if the file relating to that person is no longer active, the relevant information must be deleted.

I have drawn these concerns to the attention of the Department of the Environment, Heritage & Local Government. I understand that general legislative proposals are in train in this area and that this issue will be addressed in that context.

An Garda Síochána

In last year's report I highlighted the Code of Practice on data protection which I had concluded with An Garda Síochána (police force). The Code demonstrated that An Garda Síochána take their data protection responsibilities very seriously. This stems from a recognition that the basic principles of data protection, when applied to police work, are actually helpful rather than an impediment to the work. I am glad to say that in the past year the Gardaí have sought the views and input of my Office on a range of issues including the introduction of an Automatic Number Plate Recognition system (ANPR). These engagements have demonstrated a clear desire on the part of An Garda Síochána to meet its data protection responsibilities. I look forward to continuing contact.

An Post

As mentioned under 'Privacy Audits', my Office conducted an audit of certain data handling practices of An Post (postal authority). Of necessity the scope was limited and the audit was only able to focus on a fraction of the information held by An Post. The decision to conduct the audit was influenced by a growing unease on my part as to whether An Post had appropriate procedures and systems in place to match the type of data it holds. After all, this is an organisation with employees that call to all of our doors every day. This trusted access brings corresponding responsibility with it. I am certainly not suggesting that An Post does not take its responsibilities in relation to the confidentiality of the post seriously; on the contrary, these responsibilities are taken very seriously indeed. However, the company came increasingly to my attention as a result of its role in relation to TV Licensing and the operation of its mail redirection service. My Office was concerned that persons validly availing of the paid mail redirection service were not presented with a sufficiently prominent opportunity to refuse permission to pass their details for direct marketing purposes to third parties. Worse still, my Office received complaints during the year that the details of minors entered validly on the redirection forms were harvested and used for direct marketing purposes. Of course An Post did not know that these were the details of minors but there was no sufficiently clear information to ensure that a parent would exercise due caution when entering such details. It also became clear that any person paying An Post for this service to redirect their mail was finding their details entered on the TV

Licence database. Whatever the legal position in this respect, I considered that this practice, at best, lacked the transparency one might expect from a public agency.

In regard to the TV licence database, during the course of the year my Office received a number of complaints about personally addressed mail from An Post regarding alleged failure to have a TV licence. The people complaining were perplexed and rather irritated as to where such details were sourced. A number of them sought the source of such information from An Post which does not reveal such sources. The difficulty is that the lack of information creates a vacuum within which all manner of conspiracy theories tend to grow. The exact method of sourcing these details is of considerable concern to me and my Office continues to engage with An Post on this matter. I cannot allow the current lack of information to continue and I expect significant movement on this issue.

It is very unusual for an audit of a state entity to run into difficulty. Unfortunately An Post staff felt that there were limits to the information that my Office could access as part of the audit. There are no such limits. It was necessary to resolve this issue at a senior level in the course of the audit. While I continue to have concerns in relation to the overall approach to data protection within An Post, I am encouraged by the attention that it is now receiving at senior level in the company.

Public consultation on records held for archives & historical research purposes

The Data Protection Acts (Section 1 (3C)) provide that the normal restrictions on processing personal data (in particular the requirement that personal data should be securely destroyed when no longer required for the purpose for which it was first obtained) do not apply to:

(a) data kept solely for the purpose of historical research; or

(b) other data consisting of archives or departmental records (within the meaning of the National Archives Act 1986);

the keeping of which complies with such requirements as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of data subjects.

During 2008, my Office received an increasing amount of queries from people who were concerned that their data was available for research and from organisations, including Government Departments, who wanted clarity about data protection rights obligations in this area. I decided to start setting out requirements. These efforts produced the draft Data Protection (Archives & Historical Research) Regulations 2008 (http://www.dataprotection.ie/documents/press/draft.doc) . Their purpose is to prescribe requirements that strike a balance between the rights of individuals to control their personal data and the need for researchers and the public more generally to gain access to such data. The Director of the National Archives was involved in drawing up the draft Regulations. The Regulations are aimed at providing reassurance to individuals that personal data relating to them (retained either in records subject to the National Archives Act or retained solely for historical research purposes) will be subject to safeguards that protect their right to privacy.

The next step in the process was the launching of a public consultation process in July inviting submissions from interested parties. On foot of a number of interesting and helpful submissions I have made some further amendments which will be examined again in conjunction with the Director of the National Archives.

I intend to have the Regulations finalised during 2009 and I believe that they will benefit everyone involved in this field by providing clarity regarding their data protection responsibilities.

Health issues

The need to engage on a range of data protection issues with the health sector was, once again, a recurring theme throughout the year for my Office. This is a priority for my Office because the personal data of patients held by the health sector is clearly of a sensitive nature. I take my responsibility to ensure that this data is appropriately protected very seriously. If it is not handled with care and attention it can have grave consequences for the individuals concerned. Equally, if people do not have confidence that the health sector will protect their sensitive health data, it will not be provided in the first place. We would all suffer as a result.

Thankfully those entrusted with our health data are more than willing to engage on these issues and to ensure that sensitive health data is protected. The key players with responsibility in this area (the Department of Health and Children, the HSE, the Health Information and Quality Authority, representative bodies and individual hospitals) continue to discuss data protection issues with my Office. I welcome this but there is no room for complacency.

My Office is engaged on a range of health-related issues and I have set out a sample of these below. Despite this engagement, I am concerned that willingness to discuss the issues was sometimes not matched by effective action. I have, on occasion, discerned a view that situations exist in which the legitimate privacy expectations of patients are not a priority. Excuses may include budgetary pressures, administrative demands or research priorities. Provided appropriate measures are taken to comply with its requirements, data protection is not a barrier in any of these areas. With this in mind, I will remain vigilant to ensure that data protection rights continue to be respected.

I was disappointed on a number of occasions during the year when the HSE did not seem to be able to match its good data protection policy intentions with practice on the ground. There were a number of high profile losses of sensitive personal data by HSE employees that did not appear to demonstrate any real learning or improvement from one incident to the next. I do, of course, accept that the HSE is a large and evolving organisation and that it faces particular difficulties in reaching out to its numerous and dispersed staff. However, these factors do not release the HSE from its responsibility to ensure that it makes every effort to meet its data protection responsibilities. In this context, I found it necessary to instruct senior officials from my Office to meet with senior management in the HSE to discuss our concerns. I was gratified that, as part of that engagement, the HSE acknowledged that it holds sensitive personal information on a large part of the population and that it has important obligations in that respect. The HSE also recognised that improvements in its data handling practices were possible and, somewhat later than I might have hoped, agreed that data protection was a priority. Specifically in regard to the issue of data loss, the HSE put in place an aggressive roll-out programme for encryption of all laptops holding personal data. Additionally, HSE CEO Professor Brendan Drumm

issued a memorandum to all staff in the HSE about their data protection obligations. I welcome the HSE's practice of reporting data security breach incidents to my Office and their practice of informing everyone affected by the breach.

As I have mentioned elsewhere in this report, I have significant concerns in relation to any unjustifiable reliance upon the PPSN (Personal Public Service Number) for identification purposes. I have noticed an increasing tendency to use the PPSN in the health sector. While it is true that the HSE is permitted to seek the PPSN in the context of the provision of a service, all such requests must be justifiable. The use of the PPSN in the health sector must be strictly governed and limited in view of the serious consequences for people whose health records become easily accessible and find their way into the wrong hands. I will be following this issue closely as I cannot allow the PPSN to become the de facto health identifier just as a debate is taking place on what should become the health identifier. This debate seems to recognise that, for the reasons I have outlined, the PPSN is not a suitable tool for these purposes. I will engage closely with the HSE to ensure that all uses made of the PPSN are legitimate and justifiable and that it is not used as a de facto identifier in the health sector.

Health Information Bill

The Department of Health and Children launched discussion papers on the proposed Health Information Bill as part of a public consultation process during 2008. On foot of our formal submission, representatives from my Office met with senior officials of that Department to further discuss our views about how the legislation should be structured. The legislation has many important objectives which we believe can be delivered with due regard to privacy principles.

The approach of my Office in this area is to seek an acceptable balance between the need for health care providers to share personal health information for the care of patients and patients' right to control the use of their personal information. We look forward to undertaking further work with the Department as it develops formal legal proposals in 2009. Our response to the Department identified a number of key issues with data protection implications:

- The establishment of a specific legal structure for a national electronic health record;

- Agreement on what constitutes personal health information;
- The establishment of a Unique Health Identifier (which should not in our view be the PPSN);
- The use of personal health information in conjunction with population registries; and
- The use of personal health information for research purposes.

Our submission to the Department of Health and Children is available to view at the following link:
http://www.dataprotection.ie/docs/Submission_of_the_Office_of_the_Data_Protection_Commissioner/900.htm

National Client Index

The implementation of a national client index for the health sector has been identified as a high priority within the HSE's Transformation Programme (2007-2010). My Office was approached for views as a key stakeholder in the development process. A national client index is a system that works by first examining existing client records across multiple locations and then, using specific client matching criteria, building an index which facilitates access. This is one of several national programmes, which we have been asked to review from a data protection perspective, that propose to link up records electronically. We have tried to provide helpful advice about the data protection implications of projects of this type. We expect that the Health Information Bill should provide clarity in these areas when enacted.

International Responsibilities

Article 29 Working Party

Article 29 of the EU Data Protection Directive 95/46/EC provides for a Working Party to act as an adviser and advocate when data protection issues arise at European level. It promotes a uniform application of the provisions of the Directive throughout the European Economic Area. During the year, the Office maintained its active involvement with the Article 29 Working Party. We participated in each of the Working Party's plenary meetings as well as in a number of its sub-groups.

The Working Party made significant progress on **Binding Corporate Rules (BCRs).** BCRs are a system to facilitate the safe transfer of personal data between EU and non-EU subsidiaries of multinational companies. This is discussed further below.

The Working Party also approved position papers in regard to search engines, children's data protection, airline passenger data, EU border management, the draft revised *e*Privacy Directive and the World Anti-Doping Code draft International Standard for the Protection of Privacy. It also agreed that implementation of the Data Retention Directive 2006/24/EC would be the next area for joint enforcement activity.

All of the Working Party's documents are available on its website (http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm) .

International Data Transfers – Binding Corporate Rules

The EU Data Protection Directive and the Data Protection Acts impose conditions on the transfer of personal data to countries outside of Europe that are not considered to provide an "adequate" level of data protection. Data controllers that transfer large quantities of personal data outside of Europe must do so in accordance with the provisions of Section 11 of the Acts. To facilitate multinational companies with operations in many countries, the Working Party has developed an alternative system of "Binding Corporate Rules" (BCRs). BCRs allow the composite legal entities of a corporation (or conglomerate) to jointly sign up to common data processing standards that are compatible with EU data protection law. If they use BCRs, companies do not need individual contracts between EU and non-EU subsidiaries for the transfer of personal data between them.

I signalled previously that I hoped to see further changes in the approval process for BCRs to make them as workable as possible for business. 2008 proved to be a year of progress towards a more consistent approach to the approval process among EU Data Protection Authorities (DPAs). Previously, a BCR application had to be separately examined and approved by DPAs in every country where the business had a legal presence. This often resulted in delays. In June the Article 29 Working Party

responded to this situation by adopting a number of working documents on BCRs. These included a table with the elements and principles to be found in BCRs (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp153_en.pdf) and a framework for the structure of BCRs (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp154_en.pdf). In these documents the Working Party laid down an important foundation for further improvements to the BCR coordination procedure. These improvements were announced following a workshop for DPAs which took place in Paris in September. After this workshop a number of DPAs signed up to a mutual recognition declaration. Mutual recognition of BCRs means that, when the lead DPA circulates a draft of the BCR with a positive opinion (i.e. that it complies with all relevant documentation of the Article 29 Working Party mentioned above), other DPAs accept this opinion as sufficient basis for facilitating authorisation for the BCR in their jurisdiction. By the end of 2008, 15 DPAs had signed up to this policy commitment.

Third Pillar Groups

The formal advisory role of the Article 29 Working Party is limited to the First Pillar of the EU (also called the "Community Pillar", it concerns economic, social and environmental matters). The Office is also represented at meetings in Brussels of groups dealing with issues in the Third Pillar (the fight against crime). These groups include the EUROPOL Joint Supervisory Body (which reviews the activities of the European Police Office to make sure that its use of personal information does not violate individual privacy rights), the Customs Joint Supervisory Authority (which ensures that personal data within the European Customs Information System is processed in a manner that respects data protection rights) and the EUROJUST Joint Supervisory Body (which meets in the Hague to ensure that cross-border cooperation between EU judicial and prosecution authorities respects data protection rights).

Over the past year, these and related groups have dealt with issues such as:

- The Framework Decision on Data Protection in the Third Pillar, which was adopted by the Justice and Home Affairs Council of the EU in November 2008. This is the first general EU framework for data protection in the area of

law enforcement. Its adoption is a recognition of the importance of data protection in an area in which increasing quantities of personal data are exchanged. EU data protection authorities, including myself, are concerned to ensure adequate supervision of the implementation of the Framework Decision.

- The incorporation of the Prüm Convention into EU law. This Convention aimed to increase the exchange of information by providing a legal basis for Member States to grant each other access to their automated DNA and fingerprint identification systems and vehicle registration data. The EU's data protection authorities worked to ensure that adequate data protection controls were included in the Council Decision stepping up cross-border cooperation in this area.

- The enforcement of the right to know, and to exercise control over, how EU law enforcement cooperation agencies are using personal data. In this context the data protection authorities continue to cooperate to ensure that the EU's law enforcement agencies respect the data protection rights of individuals, including their right to access personal data held about them by these agencies. The data protection authorities also inspect databases maintained by these agencies to ensure that adequate data protection safeguards are in place.

Other international engagements

I attended the Spring Conference of European Data Protection Authorities hosted by the Italian data protection authority. The Conference considered issues such as the impact of security policies on data protection rights and the impact of new technologies on privacy.

I also participated in the 30th International Conference of Data Protection and Privacy Commissioners, jointly hosted this year by our French and German colleagues. The Conference focused on the theme of "Protecting Privacy in a Borderless World". It examined how privacy and data protection can be protected in the context of global

communication flows. It also considered the functioning of data protection law at an international level.

We also continued to follow the useful work being done in the OECD, especially in the area of cross-border enforcement of data protection.

We continue to maintain close informal contacts with other data protection authorities, particularly with the Information Commissioner's Office in the United Kingdom. I attended the annual BIDPA meeting, which provides an opportunity for data protection authorities from European common-law jurisdictions to meet to discuss new trends and best practice in data protection. This year the meeting was hosted by our colleagues from Gibraltar. The close cooperation between data protection authorities throughout these islands and beyond was given special recognition in 2008 when President McAleese hosted a reception for them in Áras an Uachtaráin. Representatives from other complaints-handling bodies, from both north and south, were also in attendance. I was pleased that the President took the decision to host this event as it served to highlight the importance of these bodies.

In April, my Office worked with our Polish data protection colleagues in a new project developed within the EU's Leonardo da Vinci Programme. The project provided an opportunity for staff of the Polish Bureau of the Inspector General for

Personal Data Protection to see how data protection legislation was applied in Ireland. Our visitors got acquainted with the day-to-day work of the Office of the Data Protection Commissioner and examined more specialized tasks undertaken by the Office. The two-week specially-tailored programme allowed each participant to focus on the areas most relevant to their work. During their stay they observed work processes, exchanged experiences and discussed data protection issues with my team. Our Polish colleagues also observed presentations and public awareness building exercises undertaken by my Office.

Administration

Running Costs

The costs of running the Office in 2008 were as follows:

	2007 (€)	**2008 (€)**	**% change**
Overall running costs	1,835,375	2,041,097	11% increase
Receipts	535,405	591,421	10% increase

Table 3 - Running costs

A fuller account of income and expenditure in 2008 is provided in Appendix 3.

Part 2

Case Studies

Case study 1: HSE West and a consultant ophthalmic surgeon breach the Acts

I received a complaint from a data subject about an alleged disclosure of personal information concerning his medical condition by a data controller. The data subject was involved in an insurance action with a third party in relation to an eye injury. The third party's insurance company requested the data subject to attend a consultant ophthalmic surgeon for an assessment at his private surgery in Limerick. The consultant was also a consultant ophthalmic surgeon at the Mid-Western Regional Hospital in Limerick. The data subject had previously attended another consultant ophthalmic surgeon at the Mid-Western Regional Hospital as a public patient in relation to his eye injury.

The complaint was two fold. The first aspect related to the alleged release of the data subject's hospital chart by the Mid-Western Regional Hospital to the consultant ophthalmic surgeon acting on behalf of the insurance company in his private practice. It was alleged that this took place without the data subject's consent. The second aspect of the complaint related to the alleged unfair obtaining of the data subject's hospital chart by the consultant ophthalmic surgeon.

The first point to be borne in mind in relation to this case was that the personal data in question, being medical records of the data subject, constituted 'sensitive personal data' as defined in the Acts. The central issue to be considered in this case, from a data protection point of view, was whether the HSE West, Mid-Western Regional Hospital complied in full with its obligations under the Acts.

Section 2 of the Acts deals with the collection, processing, keeping, use and disclosure of personal data. I was satisfied that no data protection issues arose in relation to sections 2(1)(a),(b), (c)(i), (c)(iii) or (c)(iv) of the Acts in relation to the Mid-Western Regional Hospital's collection, processing, keeping and use of the data subject's sensitive personal data. However, the disclosure of the data subject's medical chart to the consultant ophthalmic surgeon had to be considered in the context of section 2(1)(c)(ii) of the Act. This section provides that personal data should not be further processed in a manner incompatible with the purpose for which it was collected. It was clear from my Office's investigation that the consultant

ophthalmic surgeon's secretary at his private rooms contacted his secretary at the Mid-Western Regional Hospital to locate the data subject's medical records relating to his eye condition. Following this contact, the secretary based at the hospital located the record and disclosed it to the consultant surgeon's private surgery.

In assessing this issue from a data protection perspective, a clear distinction must be drawn between the consultant surgeon's work within the HSE West, Mid-Western Regional Hospital as an employee of that hospital and his work carried out privately on behalf of an insurance company. The hospital's disclosure of the medical records to the private rooms of the consultant surgeon undoubtedly involved the disclosure of those records from one data controller (the HSE West, Mid-Western Regional Hospital) to another (the consultant surgeon's private surgery). It could not be regarded as information sharing within a single data controller because the consultant surgeon sought the data subject's medical record from the hospital in his capacity as a separate data controller. In this instance he was not acting in his capacity as an employee of the HSE.

The medical record at the Mid-Western Regional Hospital in respect of the data subject was compiled in the course of his treatment for an eye condition. This was a specific, explicit and legitimate purpose. Any further use or disclosure of that medical record must be necessary for that purpose or compatible with the purpose for which the hospital collected and kept the data. The consultant surgeon was a separate data controller who sought this data for the purposes of an assessment of the data subject's eye condition on behalf of an insurance company to facilitate their processing of an insurance claim. The processing of an insurance claim related to the data subject's eye injury represented an entirely different purpose to the treatment of the data subject for an eye condition at the Mid-Western Regional Hospital.

There was also an obligation to meet the conditions set out in Section 2A of the Acts. These conditions included obtaining the consent of the data subject or deeming that the processing of the data was necessary for one of the following reasons:

- the performance of a contract to which the data subject is a party;

- in order to take steps at the request of the data subject prior to entering into a contract;
- compliance with a legal obligation, other than that imposed by contract;
- to prevent injury or other damage to the health of the data subject;
- to prevent serious loss or damage to property of the data subject;
- to protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged;
- for the administration of justice;
- for the performance of a function conferred on a person by or under an enactment;
- for the performance of a function of the Government or a Minister of the Government;
- for the performance of any other function of a public nature performed in the public interest; or
- for the purpose of the legitimate interests pursued by a data controller except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

In this case, the data subject did not give his consent to the Mid-Western Regional Hospital for the processing of his personal data involving the disclosure of his medical record to the consultant surgeon. In the absence of consent, the data controller must be able to meet at least one of the eleven conditions set out above. In this instance, the hospital did not meet any of those conditions.

To process sensitive personal data, in addition to complying with Sections 2 and 2A of the Acts, at least one of a number of additional special conditions set out in Section 2B(1) of the Acts must be satisfied:

- the data subject must give explicit consent to the processing or
- the processing must be necessary for one of the following reasons:
    - for the purpose of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;

- to prevent injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where consent cannot be given or the data controller cannot reasonably be expected to obtain such consent;
- it is carried out by a not-for-profit organisation in respect of its members or other persons in regular contact with the organisation;
- the information being processed has been made public as a result of steps deliberately taken by the data subject;
- for the administration of justice;
- for the performance of a function conferred on a person by or under an enactment;
- for the performance of a function of the Government or a Minister of the Government;
- for the purpose of obtaining legal advice, or in connection with legal proceedings, or for the purposes of establishing, exercising or defending legal rights;
- for medical purposes;
- for the purposes of political parties or candidates for election in the context of an election;
- for the assessment or payment of a tax liability; or
- in relation to the administration of a Social Welfare scheme.

As stated previously, the consent of the data subject, explicit or otherwise, was not obtained by the data controller for the processing of his personal data involving its disclosure by the Mid-Western Regional Hospital to the consultant surgeon. There are twelve conditions set out above, at least one of which must be met by a data controller in the absence of explicit consent before sensitive personal data can be processed. In this instance, the Mid-Western Regional Hospital did not meet any of those conditions.

I formed the opinion that the HSE West, Mid-Western Regional Hospital contravened Section 2(1)(c)(ii), Section 2A(1) and Section 2B(1)(b) of the Acts by processing the

data subject's sensitive personal data in a manner which was incompatible with the purpose for which it was obtained. This processing occurred when the consultant surgeon's secretary at the Mid-Western Regional Hospital disclosed the data subject's hospital medical file to his private practice secretary. In response to this incident the HSE West put in place improved controls for ensuring that requests for access to hospital files are justified and fully in line with the purpose for which health data is held. I welcome this.

I also considered whether the consultant surgeon had breached the requirements of the Acts by obtaining and using the file created in the Mid-Western Regional Hospital.

In light of my previous decision which found a number of contraventions of the Acts by the HSE West, it followed that the consultant surgeon unfairly obtained the data subject's hospital file. However, it was also clear that this was done unintentionally and in good faith.

I accept that the lines can be blurred in some instances in the health sector between treatment provided by the public system and treatment provided by the private system (especially here in Ireland due to the public/private sector split). This can give rise to complexity in terms of data protection responsibilities as patient information flows between the public and private systems. However, no such complexity arises in relation to the transfer of personal data that is not related to the treatment of a patient (in this particular instance carried out on behalf of an insurance company). Organisations entrusted with personal data, and especially those holding sensitive personal data such as health information, have onerous responsibilities under the Data Protection Acts. These responsibilities reflect the position of trust afforded to such data controllers when they are given our personal data.

Case study 2: Disclosure of email addresses by a financial institution

In April 2008, I received a complaint from a data subject whose email address had been disclosed by a financial institution. The disclosure took place when the financial institution issued an email to 114 individuals with the email addresses of each of them visible to all recipients.

The background to this incident was that the data subject received several phishing emails. Having consulted the relevant financial institution's website, he reported the matter using an email address provided by the financial institution for that purpose. Generally, phishing emails concerning banking services give the impression that they have been issued by a bank. They often request the recipient to log-on to their online banking service to confirm their security details by clicking the link in the email. If a person clicks on that link they are routed to a 'spoof' site which looks like the bank's online service. The intention of the fraudster is that the recipient will be fooled into disclosing their confidential details to the 'spoof' site.

The matter of the disclosure of the data subject's email address was raised by my Office with the financial institution. It explained that when an email is received by the team which handles reported instances of phishing a standard response is sent advising the user of additional precautions to take and providing related information. However, on a particular weekend in April 2008, an unprecedented number of emails were sent to the phishing alert email address. To respond to each email a business decision was made to send a single response to all customers using the "bcc" (blind copy) option in e-mail, which would have hidden all email addresses from the recipients. This bulk email failed because it was too large. To make the email more manageable for the mailbox, the user list was broken down into different outgoing emails. Due to a manual error, one of the emails was sent to 114 people using the "cc" option rather than the "bcc" option. This resulted in all 114 email addresses being visible to all recipients of the email.

The financial institution subsequently issued an email to the affected users to advise them of the incident and to apologise for the error. I am satisfied that the financial institution took prompt action to inform the affected parties that their email addresses

had been disclosed. However, it is unfortunate that this disclosure occurred in the context of an email alert system that was established to prevent phishing.

All data controllers should take note of this incident and take steps to ensure that email addresses are not disclosed inadvertently. In particular, where an email is sent to a number of individuals it should be transmitted using the blind copy ('bcc') option in all situations which warrant it. **It is the duty of data controllers to raise awareness amongst their employees about this issue and to foster a greater degree of care and responsibility in relation to the protection of personal data in the form of email addresses**. However, I have some sympathy for data controllers where genuine mistakes occur in this area.

Case study 3: A marketing campaign sets up personalised website addresses and breaches the Acts

During the summer of 2008 I received three complaints from data subjects concerning a marketing postcard campaign launched by 123.ie to promote its home insurance product. The complainants had no previous business dealings with 123.ie and they expressed surprise at receiving personally addressed marketing mail from this source. An unusual aspect of this marketing campaign involved the creation of personalised URLs (website addresses). Each postcard included details of a personalised URL set up in the name of the recipient. When the recipients logged-on to their personalised website address they were invited to input their email address details and phone numbers.

The establishment of URLs using people's names without obtaining their consent was a concern from a data protection perspective. In addition, there was no evidence that 123.ie had made any attempt to comply with the 'fair processing' requirements set out in section 2D of the Data Protection Acts. For that reason, my Office informed 123.ie that the establishment of personalised website addresses (or URLs) in this manner was a breach of the Acts. Printing the URL on a postcard and distributing it in the postal system was a disclosure of personal information and a further breach of the Acts. Furthermore, the collection of email addresses and phone numbers when the recipient logged on to the URL failed to meet the requirements of fair processing because no information was provided to those individuals about the purposes of collecting the information.

On receiving the complaints my Office immediately contacted 123.ie requesting that it disable the relevant personalised URLs. 123.ie cooperated with my Office on this matter and reverted without delay confirming that the URLs relating to each complainant had been disabled.

At the request of my Office 123.ie confirmed that:

- it would not undertake such a campaign again;
- that it had not used and would not use any of the information obtained from potential customers as a result of this campaign; and

- that it had disabled all URLs which incorporated individual names relating to this campaign.

Prior to my Office's receipt of the individual complaints referred to above, 123.ie informed my Office that it had discovered that minors had been targeted in its postcard campaign in error. 123.ie informed us that it worked with a creative agency (New Oceans) and a data agency (Data Ireland) in the execution of its postcard campaign. Data Ireland is a subsidiary of An Post. It subsequently emerged that the names and addresses of the minors targeted during this postcard campaign were originally drawn from the An Post Movers file. My Office is actively communicating with An Post on this matter to ensure that further breaches of the Acts do not occur in relation to the use of databases held by An Post and in particular where those databases contain the details of minors. My Office views the inappropriate use of the personal data of children as a particularly serious breach of the Data Protection Acts.
.

Case study 4: Interactive Voice Technologies and unsolicited text messages

During the latter half of 2006 a mobile phone service provider informed me of the receipt of a number of unsolicited premium rate text messages by two of its customers relating to adult content subscription services. The messages were sent by Interactive Voice Technologies (IVT) and one of the recipients was a minor. Both recipients denied that they were existing or previous customers of IVT and they stated that they did not consent to receiving any of the messages.

When my Office investigated this matter, it was found that both mobile phone numbers had been recycled (this is the industry term to describe the re-use of a mobile number when it has been out of use for a period of time, usually one year). The numbers were allocated to the new users when they opened their mobile phone accounts. It was the new users who received the unsolicited text messages. We were told by IVT that both mobile numbers had entered its database when the original owners (before recycling) had subscribed to its service. Due to a technical error its systems did not detect that the numbers were recycled, resulting in both new users receiving content when the numbers were reactivated.

My Office communicated my concerns to IVT that its systems did not appear to be sufficiently robust to prevent adult content material being sent inadvertently to a recycled number. Furthermore, since neither individual could have legitimately consented to receiving the text messages, I considered that the messages were unsolicited for the purposes of direct marketing and in direct contravention of Regulation 13 of Statutory Instrument 535 of 2003. IVT argued that it was not its intention to send messages to the new users because, as far as its systems were concerned, it was still providing a service to the original customers.

My Office advised IVT, as the data controller, that it would have to take immediate corrective action to satisfy me that it was taking its data protection responsibilities seriously. I encouraged IVT to consider settling this matter by way of an amicable resolution. This was an appropriate solution for a company that has proved compliant with data protection requirements in all other respects. The company, having considered the matter, agreed to refund the charges incurred by both individuals in

respect of the premium rate text messages and to offer their written apologies to both individuals. As a gesture of goodwill, IVT agreed to purchase two kidney dialysis machines for donation to Temple Street Children's' Hospital at a cost of over €27,000.

Given the issues surrounding the sending of adult content messages to recycled mobile phone numbers (including to the phone number of a minor) we referred these to the Communications Regulator(ComReg) for examination. I was subsequently advised by ComReg that it had been decided to extend the quarantine period for recycled numbers from six months to twelve months. Comreg also decided to request mobile network operators to advise service providers using their networks when a mobile phone number was placed in quarantine.

This case demonstrates the high risk associated with sending of marketing messages or premium rate services to mobile phone numbers which have been recycled. It is unacceptable that extra steps were not taken to ensure that adult content was not being sent to the mobile phone of a minor. Those engaged in the sending and promotion of adult content to mobile phones should take note of this case and ensure they take appropriate measures to comply, not only with their data protection obligations, but also with their obligations under other legislation. On an overall basis, I welcome the constructive approach to this issue and the amicable resolution. This is a good indicator of how seriously IVT took this issue.

Case study 5: Unfounded complaint about unsolicited marketing text messages

My Office received a complaint from a data subject about text messages that she had received to her mobile broadband modem. The data subject first found out about the text messages when she received her mobile broadband bill. Over a two month period she had incurred charges amounting to hundreds of euro for premium rate text messages.

My Office investigated the complaint on the basis of the data subject's allegation that the messages were unsolicited. On investigating the complaint, my Office found that the data subject's broadband bill showed that she had been charged for premium rate text messages by four separate data controllers. It was then established with the data subject's mobile network provider that her mobile broadband modem was capable of sending and receiving text messages. It confirmed that this was technically possible and that mobile broadband modems have SIM cards with mobile phone numbers assigned to them.

My Office then contacted the relevant data controllers to find out where they had sourced the data subject's mobile number and whether they had obtained appropriate consent to send her the text messages. Each of the data controllers responded promptly with full details of all messages sent to, and received from, the data subject's mobile number. These responses indicated that the communications had been initiated from the data subject's mobile number. My Office then compared these details with the data subject's broadband bill which confirmed the data controllers' version of events. Following a detailed examination of the case and taking account of the material submitted by all four data controllers, I was satisfied that the text messages were not unsolicited and that no contraventions of SI 535 of 2003 had occurred. It became apparent that a member of the data subject's household had subscribed to the relevant services using the data subject's mobile broadband modem without her knowledge. This was not the fault of the data controllers.

Similar situations arise quite often in regard to complaints to my Office about subscriptions to phone services. **It is not uncommon to find that another member of the complainant's household, such as a child or spouse, has used the mobile**

phone of the complainant without their knowledge to subscribe to various services.

Case study 6: Total Fitness Ireland and legal powers used to ensure compliance with an access request

In December 2007 I received a complaint from a data subject regarding a refusal by Total Fitness Ireland to comply with his access request. One day after the submission of his access request, Total Fitness Ireland informed the data subject in an email that it was not prepared to give him access to records related to his membership. . However, it did not claim any of the limited exemptions to the right of access under the Data Protection Acts. Where a data controller refuses to comply with an access request it must notify the data subject and explain the reasons for refusal in accordance with the exemptions in the Acts. The data controller must also inform the data subject that they may complain to the Data Protection Commissioner about the refusal.

My Office commenced an investigation of the complaint by writing to Total Fitness Ireland. However, Total Fitness Ireland failed to respond to any of our letters, emails or phone calls. In effect, it failed to cooperate with my statutory investigation. For this reason I served an Enforcement Notice on Total Fitness Ireland in March 2008 pursuant to section 10 of the Acts. The Enforcement Notice was served on the basis that I believed that Total Fitness Ireland had not complied with an access request and was therefore in contravention of Section 4 (1) of the Acts. An Enforcement Notice is a legal notice that must either be complied with within twenty one days or be appealed to the Circuit Court. Failure to comply with an Enforcement Notice is an offence liable to a fine on summary conviction in the District Court of €3,000. Total Fitness Ireland was required to comply with the terms of the Enforcement Notice by providing the data subject with a copy of all of the personal data that he sought, subject to any exemptions which it could legitimately claim under the Acts.

Total Fitness Ireland responded to the Enforcement Notice by informing my Office that the file records which it held in regard to the data subject related only to his health club membership. Copies of these records were given to him on the date he commenced his membership and when he subsequently renewed it. In response, my Office told Total Fitness Ireland that we were aware, on the basis of information supplied to us by the data subject, that it held other information relating to the data

subject in respect of comments and complaints made by him. My Office also pointed out to Total Fitness Ireland that the issue of whether the data subject was already in possession of copies of his health club membership records was not relevant to their compliance with the access request. We clarified that copies would have to be provided to him in response to his access request.

My Office subsequently received a letter from Total Fitness Ireland concerning the Enforcement Notice. In this letter, Total Fitness Ireland challenged the statement in the Enforcement Notice that it was in breach of section 4(1) of the Data Protection Acts. Among other things, Total Fitness Ireland stated that there was no valid access request from the data subject because it claimed that the data subject had made his request verbally and not in writing as required by the Acts. Total Fitness Ireland also claimed that a copy of the data subject's file was made available to him in response to his verbal request. The file contained a copy of the data subject's agreement with Total Fitness Ireland and correspondence related to the renewal of his membership. This was all the personal data it held relating to the data subject. On this basis, Total Fitness Ireland sought the cancellation of the Enforcement Notice.

My Office contacted the data subject who confirmed that he had submitted his access request in writing by registered post to Total Fitness Ireland. The data subject had also received from Total Fitness Ireland a scanned copy of his access request as an attachment to the initial email which it had sent to him refusing him access to his data. In view of this my Office told Total Fitness Ireland that I would not cancel the Enforcement Notice.

I considered that the situation that had arisen was unacceptable. I instructed two of my authorised officers, using the powers conferred on them by Section 24 of the Data Protection Acts, to visit the premises of Total Fitness Ireland in Castleknock. Total Fitness Ireland cooperated with the inspection. My authorised officers found a copy of the data subject's written access request as well as a significant amount of personal data relating to the data subject. None of this data had been supplied to him.

On the basis of the inspection, my Office informed Total Fitness Ireland's solicitors that we were completely satisfied that their client had breached both sections 4(1) and

4(7) of the Acts concerning the data subject's access request. Their client had also committed an offence by failing to comply with an Enforcement Notice. The Acts mandate me, in certain circumstances, to try to reach an amicable resolution to a complaint. Soon afterwards, an amicable resolution was achieved. Total Fitness Ireland provided the data subject with copies of all the personal data it held relating to him. The company apologised to the data subject for failing to provide the personal data on time and for the inconvenience caused to him as a result. As a gesture of goodwill, Total Fitness Ireland donated a sum of €300 to a charity of the data subject's choice.

I was satisfied with the overall outcome of this complaint. However, it is unacceptable that a data controller would ignore correspondence and phone calls from my Office in the course of the investigation of a complaint. I use my legal powers sparingly but, in this case, I felt it necessary to use two separate legal powers in an effort to uphold the rights of the data subject. Had this access request been handled correctly by the data controller, the matter could have been resolved within a short time. In the course of their inspection my authorised officers found that the personal data was readily available on the computer of the data controller. It could easily have been copied and prepared for issue to the data subject with less than one hour's work. Instead, for reasons that I believe related to unhappiness about a customer service complaint, the data controller chose to refuse the request and to show disregard for my Office's investigation. **I will not accept this attitude from any data controller. Thankfully, I do not encounter such attitudes on a regular basis. However, as this case demonstrates, I will use my legal powers without hesitation if it is necessary for the investigation of a valid complaint to my Office**.

Case study 7: Opt-In to subscription service text messages found following investigation

In April 2008 I received a complaint from a data subject that she had received and had incurred charges related to subscription service text messages. The data subject received two text messages from a company on different dates early in April 2008. In her complaint to my Office, the data subject claimed to have no knowledge of opting-in to the receipt of text messages from the company.

Under Regulation 13(1)(b) of SI 535 of 2003 a person is prohibited from sending direct marketing text messages to a subscriber unless the subscriber has consented to the receipt of such communications. On the basis of the complainant's allegation that the text messages were unsolicited, I commenced an investigation of the complaint.

During the investigation my Office established that the company had obtained the data subject's mobile phone number when it was entered into one of its websites for a chance to win free flights. After the number was input into the website, a text message was sent to the mobile phone number that included a pin number. That pin number was then entered into the website to verify the subscription. Information published on the website indicated that the service was a subscription service and it outlined the cost and frequency of the subscription element. It also gave clear instructions on how to unsubscribe from the service.

I was satisfied that the company had clearly indicated on its website that the service was a subscription service for which charges would be incurred. It provided sufficient information to my Office to verify that the mobile phone number had been opted-in to receive subscription service messages. I was satisfied that the data subject had not received unsolicited marketing text messages but that she had legitimately received subscription service text messages on foot of opting-in to a service via a website. I was also satisfied that the company had put in place appropriate procedures to ensure that numbers entered on the website were validly entered. I do not accept claims of valid consent based solely on the fact that a number was collected after it was typed on a website. That does not constitute a valid consent. In this case, the individual

receives a subsequent text message to which they must respond and actively opt-in, thus removing any doubt about the validity of the consent.

This case study is a clear reminder that data subjects need to pay greater attention to information that is made available to them in relation to entering services, competitions, etc., particularly on websites. In this case the data controller provided comprehensive information on its website in relation to the service that the data subject chose to enter. Yet, when the data subject began to receive text messages in respect of the service over the following few days, she claimed to have no knowledge of opting-in to the service. **In light of our investigation, there were no grounds for upholding her complaint against the data controller.**

Case study 8: BuyAsYouFly and a failure to respect opt-outs from direct marketing by email

I received a complaint from a data subject regarding direct marketing emails she had received from BuyAsYouFly.com. The complainant provided my Office with copies of several of the marketing emails that she had received from the company as well as copies of her attempts to unsubscribe. It was clear from an initial examination of this material that she had followed the 'opt out' instructions contained in the emails but, in spite of that, she continued to receive the unwanted emails. I was particularly concerned about the number and frequency of emails that she continued to receive after her efforts to unsubscribe. On examination of the complaint, it appeared that the company was committing offences by failing to record the opt-out preference of the complainant and by continuing to send the complainant direct marketing emails, contrary to the provisions of S.I. 535 of 2003.

My Office commenced an investigation of this matter. We requested that BuyAsYouFly immediately delete the complainant's email address from its marketing database. We also sought an explanation as to why her unsubscribe requests were not respected by the company.

BuyAsYouFly responded by advising that it had suffered a serious systems error which resulted in loss of data. As a result the company unintentionally continued to use an older version of its database. The company removed the complainant's email address from its database and it agreed to suspend outbound emails until its unsubscribe lists were fully reconciled with the database. It conveyed an apology to the complainant and, as a gesture of goodwill, it offered the complainant a gift to the value of €100 from its online shop. This was accepted by the complainant as an amicable resolution of her complaint.

I was satisfied with the corrective measures taken by BuyAsYouFly to resolve this complaint and to prevent any recurrence. **This case highlights the obligations imposed on marketers to ensure that they respect the preferences of the general public who do not wish to receive marketing communications. This is even more**

important when the person makes efforts to refuse the receipt of further communications.

Case study 9: An access request and a successful claim of legal privilege by a Data Controller

In May 2007 I received a complaint from a solicitor acting on behalf of a client regarding the alleged failure of a data controller to respond to an access request. The solicitor had submitted an access request on behalf of his client to her former employer in February 2007. The data controller failed to respond to the access request within the statutory forty-day period.

My Office commenced an investigation by writing to the data controller about the complaint. We received a reply from the data controller's solicitor confirming that a response had issued to the access request. The reply included a number of documents containing personal data. However, the data controller's solicitor informed my Office that their client was claiming privilege in respect of two specific documents and was therefore not releasing them. These documents were a handwritten account by the store manager of the data subject's period of employment with the data controller and a handwritten account by the store manager relating to the data subject's alleged personal injuries suffered as a result of a workplace accident in July 2006. The solicitors for the data controller informed my Office that both documents were created by their client for the benefit of legal advisers and in anticipation of litigation following receipt of two solicitor's letters on behalf of the data subject.

There are some very limited exemptions within the Data Protection Acts to a data subject's right of access. These are set out in Sections 4 and 5 of the Acts. One of the restrictions to the right of access is set out in Section 5(1)(g). This states:-

Section 4 of this Act does not apply to personal data in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his professional legal advisers or between those advisers.

The data subject's solicitor subsequently informed my Office of his dissatisfaction with the data controller's claim of privilege. It was necessary for my Office to be satisfied that the data controller's claim of privilege in relation to these documents was properly founded. For that purpose I requested the data controller to confirm to my

Office the date(s) on which the documents were created and the purpose or purposes for which the documents were created. In response, we were informed that the relevant documents were created on two separate dates in the second half of February 2007 after the data controller received letters dated 6 February, 2007 from solicitors for the data subject. The data controller's solicitors informed my Office that the letters from the data subject's solicitors had intimated personal injuries and employment claims on behalf of the data subject.

The claim of legal privilege under the Acts relates only to communications between a client and his professional legal advisers or between those advisers. The date of creation of the documents, on which the data controller was claiming privilege, when compared with the dates of its receipt of communications from the data subject's solicitors, satisfied my Office about the purpose of these documents. **We accepted that the claim of legal privilege could be applied to both documents as it fell into the category of a communication between a client and his professional legal advisers.**

There are limited exemptions under the Acts to a data subject's right of access. **When a data controller claims an exemption, my Office may request additional information from the data controller to be satisfied that the withholding of the documentation is properly founded. Such matters are dealt with by my Office on a case by case basis.**

Case study 10: An employer attempts to use CCTV for disciplinary purposes

In February 2008 I received complaints from two employees of the same company regarding their employer's intention to use CCTV recordings for disciplinary purposes.

In this case, the employer had used CCTV images to compile a log that recorded the employees' pattern of entry and exit from their place of work. The employer then notified a trade union representative that this log would be used at a disciplinary meeting. It also supplied a copy of the log to the union representative. The employer sent letters to each employee requesting that they attend a disciplinary meeting to discuss potential irregularities in their attendance. The letters indicated that this was a very serious matter of potential gross misconduct and that it could result in disciplinary action, up to and including dismissal.

The employees immediately lodged complaints with my Office. They stated that they had never been informed of the purpose of the CCTV cameras on the campus where they were employed. They pointed out that there were no signs visible about the operation of CCTV. On receipt of the complaints, my Office contacted the employer and we outlined the data protection implications of using CCTV footage without having an appropriate basis for doing so. We informed the company that, to satisfy the fair obtaining principle of the Data Protection Acts with regard to the use of CCTV cameras, those people whose images are captured on camera must be informed about the identity of the data controller and the purpose(s) of processing the data. This can be achieved by placing easily read signs in prominent positions. A sign at all entrances will normally suffice. If an employer intends to use cameras to identify disciplinary (or other) issues relating to staff, as in this instance, staff must be informed of this before the cameras are used for these purposes.

The employer accepted the views of my Office. It informed the two employees that it was not in a position to pursue the matter of potential irregularities in attendance as it could not rely on CCTV evidence obtained in contravention of the Data Protection Acts.

This case demonstrates how data controllers are tempted to use personal information captured on CCTV systems for a whole range of purposes. Many businesses have justifiable reasons, related to security, for the deployment of CCTV systems on their premises. However, any further use of personal data captured in this way is unlawful under the Data Protection Acts unless the data controller has made it known at the time of recording that images captured may be used for those additional purposes. Transparency and proportionality are the key points to be considered by any data controller before they install a CCTV system. Proportionality is an important factor in this respect since the proposed use must be justifiable and reasonable if it is not to breach the Data Protection Acts. **Notification of all proposed uses will not be enough if such uses are not justifiable**.

Substantial guidance is available on our website in relation to the use of CCTV in a business or in a workplace. I would encourage all data controllers, particularly those who may already have such recording systems in place, to familiarise themselves with our guidance on this important issue.

Case study 11: Marketing telephone calls to numbers on the NDD Opt-Out Register

The marketing activities of Celtic Water Solutions came to the attention of my Office in January 2008. I received complaints from two individuals who received marketing telephone calls from Celtic Water Solutions even though they had registered their preferences not to receive marketing calls on the National Directory Database (NDD) opt-out register. This is the register of all the phone and fax numbers that have been opted out of receiving marketing calls or faxes.

When my Office investigated the matter it found that the data controller was unaware of its obligations in relation to the NDD opt-out register. **However, ignorance of the law is no excuse for breaching it. All data controllers have a responsibility to ensure that they are aware of and compliant with all of their data protection obligations.**

My Office ordered the company to cease all telemarketing activities with immediate effect and not to resume such activities until such time as it was in a position to comply with preferences recorded on the NDD opt-out register. We also sought an undertaking from the company that all future marketing calls would comply with the requirements of the law with regard to the NDD opt-out register. The company complied immediately and it ceased all telemarketing activity. It also wrote letters of apology to the complainants and it made a goodwill gesture in the form of gift tokens to each complainant. The complainants accepted the letters of apology and the goodwill gesture as an amicable resolution of their complaints to my Office.

I welcome the swift remedial action taken by the company in response to these complaints. I note in particular that the issues were resolved to the satisfaction of the complainants within a relatively short period of four weeks following the receipt of the complaints by my Office.

Case study 12: Credit unions transmitting personal data via unsecured e-mails

I received complaints from two individuals concerning e-mails they had received from two credit unions confirming details about online access to their accounts.

My Office contacted both credit unions for their views on the matter. It transpired that both credit unions were using the same third party vendor to supply their online account facilities.

When a customer registered to use the online facility, they received a confirmation e-mail that contained details about their account, including username, account number and password. A separate letter was sent to their home giving them a PIN number which would allow them to get online access to their credit union account.

Section 2 (1) (d) of the Acts requires that adequate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network. My Office entered into discussions with the third party vendor to address this issue.

The vendor's initial concern was that when people registered, they would not remember their account details when they went to log on to the system at a future date and for this reason they were e-mailing the account details to the customers. As a solution, my Office proposed that when a customer was registering they should be encouraged to print off or otherwise record the details. This would eliminate the need to have confidential information transmitted to them via an unsecured e-mail.

The third party vendor agreed to change its systems to reflect this and to inform all of its clients that it was changing its systems for security reasons.

My Office was also concerned that one of the credit unions was using a free web-based e-mail service as a method of communicating with its customers. My Office took the view that this mode of communication was not adequately secure because the data controller could not adequately control access to the contents of such an e-mail

account. The data controller had no record of access to the e-mails, even within their own organisation. My Office instructed the credit union concerned to stop using the free web-based e-mail account as a method of contacting customers. The credit union responded promptly and it changed its email to a more secure system.

This case highlights the need for all data controllers to be aware of the need for appropriate security when processing personal data. If there is a weakness in security, the matter needs to be addressed and a more secure method of providing the service must be established. **Although I understand that the purpose of credit unions is to provide services to the community in a cost effective manner, this does not in any way exempt them from ensuring that appropriate steps are taken to protect customer data.**

Case Study 13: Retention of personal data provided online

In January 2008, I received a complaint from a data subject in relation to the retention of his personal data by Ticketmaster. The data subject had provided his credit card details and his email address to Ticketmaster for the purpose of a particular transaction in 2006. However, in October 2007 and January 2008 he received emails from Ticketmaster regarding the cancellation of a concert for which he had not purchased a ticket. The data subject was concerned that his personal data had been retained by Ticketmaster for such a long time. He asked Ticketmaster to remove his details from its database and, at the same time, he complained to my Office.

On receipt of the complaint, my Office commenced an investigation into the matter. Ticketmaster holds an extensive amount of personal data including credit card details. At the outset we were concerned that the organisation might not have appropriate procedures in place for deleting personal data when no longer required for the purpose for which it was given. A subsequent response from Ticketmaster stated that the emails sent to the data subject were customer service emails regarding the cancellation of an event rather than marketing emails. I accepted this. It explained that the first email was sent in error and that the purpose of the second email was to inform the recipient that the previous email had been sent in error and that he should ignore or delete it if he had not purchased tickets to the event in question. Ticketmaster informed us that steps had been put in place to ensure that such an error would not occur again and it wrote to the data subject to confirm that it had deleted all of his personal data from its records in accordance with his request.

In the course of the investigation my Office requested a copy of Ticketmaster's data retention policy and highlighted issues in relation to the privacy policy statement on its website. Having reviewed Ticketmaster's privacy policy we found that it referred to UK data protection legislation and made no reference to Irish data protection legislation. As Ticketmaster is registered in Ireland, we considered it appropriate that a data protection notice relevant to Ireland should be published on its website.

In its response, Ticketmaster provided my Office with a detailed account of the type of personal data it collects, the purposes for which it is used and the retention policy

for such data. In relation to its privacy policy statement lacking a data protection notice for Irish customers, Ticketmaster indicated that the omission was an oversight on its part and it supplied my Office with a copy of a draft privacy policy statement for Irish customers. Ticketmaster also informed my Office that it only sends performer alert emails to customers who have previously bought tickets and that such emails are only sent in respect of "similar products or services" as they notify customers of future performances by artists for whom they had previously bought tickets. It also pointed out that Ticketmaster offers the customer in each message an easy and free opt-out from receiving future messages. My Office was still concerned about the length of time Ticketmaster retained personal data such as credit card details. Ticketmaster informed my Office that it retained personal data for sixteen months. However, my Office considered that twelve months was a more appropriate retention period and it advised that, if there was no activity on a customer's account during that time, all details should be deleted. In relation to the storage of customers' credit card details, we advised that it would be more appropriate for customers to opt in to have their details retained rather than the existing practice of requiring a customer to uncheck a box when he or she purchases a ticket. Ticketmaster agreed to implement my Office's recommendations.

I am satisfied that Ticketmaster takes its data protection responsibilities seriously and I was encouraged by the cooperative manner in which it addressed the issues and implemented my Office's recommendations.

It is important that data controllers who process personal data via websites are fully aware of their obligations in relation to personal data. Websites with customer interfaces should clearly outline to potential customers how their personal data will be processed in future and for how long it will be retained. No data subject should be surprised to find that their personal data continues to be processed long after initially inputting their information on a data controller's website.

Case study 14: Credit union commits several breaches by failing to update a member's address record.

In March 2008 I received an unusual and complex complaint against Halston Street Credit Union. The Credit Union had sent correspondence for the complainant's ex-wife to the complainant's address. After receiving the registered correspondence at his home address, the complainant informed the Credit Union by phone that his ex-wife did not reside at his address, nor indeed had she ever resided at that address. In fact they had been living apart for twenty-two years. Despite this, two further pieces of correspondence from Halston Street Credit Union to his ex-wife arrived at the complainant's address on separate dates.

My Office wrote to Halston Street Credit Union in early April 2008 informing it that we were commencing an investigation of this complaint. The complainant was anxious to establish what personal data the Credit Union held in relation to him. He was genuinely concerned that the correspondence he was receiving was prompted by fraudulent use of his personal data by a third party. We advised him to submit a request to the Credit Union under section 3 of the Acts. Section 3 of the Acts provides that an individual may submit a request in writing to a data controller to be informed whether the data controller keeps personal data relating to the individual. If the data controller does have such data, section 3 provides that the data subject should be given a description of the data and the purposes for which it is kept. Under the provisions of the Acts a data controller must respond to such a request within twenty one days. The complainant took our advice but unfortunately did not receive a response from Halston Street Credit Union to the section 3 request that he submitted in mid-July 2008.

Halston Street Credit Union failed to reply to my Office's initial correspondence despite three separate reminders during the period April to July. One of my officials received a very unsatisfactory call from one of the elected members of the Credit Union which did not provide any response to the issues raised. This situation, coupled with the failure by the Credit Union to meet its statutory obligation to respond to the request under section 3 of the Data Protection Acts, led my Office to form the view that the Credit Union had little regard either for the data protection

rights of the complainant or for my Office. For these reasons I instructed two of my senior officers, using the powers conferred on them by section 24 of the Data Protection Acts, to enter and inspect the premises of Halston Street Credit Union to obtain information relevant to the investigation of this complaint. In the course of their inspection, my authorised officers found records which confirmed that the complainant had indeed informed Halston Street Credit Union in June 2007, as he had indicated, that his ex-wife did not live at his address. No action had been taken by the Credit Union on foot of this information in terms of updating the address on file and, as a result, the complainant's address was used on two further occasions by the Credit Union to send letters intended for his ex-wife. My authorised officers also found the section 3 request that the complainant had submitted in July 2008 on the premises. They confirmed that the Credit Union had not taken any action in response to the request.

Subsequent to the inspection by my authorised officers, Halston Street Credit Union confirmed to my Office that a response issued to the complainant's section 3 request in mid-September 2008. This was over five weeks outside the statutory requirement. My Office was disappointed to discover that the Credit Union had copied its response to the section 3 request to four separate third parties. The complainant was entitled to have his request handled in a confidential manner. It was, to say the least, very disappointing that the Credit Union copied the response to the request to third parties who had no business in relation to it.

Following my Office's investigation, we found Halston Street Credit Union to be in breach of section 3(b) of the Data Protection Acts for failing to respond to the complainant's section 3 request within the statutory timeframe of twenty one days. We found that the Credit Union was also in breach of section 2(1)(d) of the Acts for its unauthorised disclosure of the complainant's personal data to third parties when responding to his section 3 request. The records of Halston Street Credit Union showed that the complainant first contacted it by telephone in June 2007 to inform it that his ex-wife did not live at his address. The Credit Union's subsequent failure to take action to remove the complainant's address from its records led it to process the complainant's personal data on two further occasions, constituting two additional breaches of his data protection rights under section 2A of the Acts. The failure of

Halston Street Credit Union to remove the complainant's address from his ex-wife's records caused two further breaches. This time the Credit Union breached the data protection rights of the complainant's ex-wife, because it sent her personal data on two occasions in August 2007 and September 2007 to an address which it knew from June 2007 to be incorrect.

The sequence of events that culminated in my instruction to my authorised officers to use their powers under Section 24 of the Acts to progress the investigation of this complaint demonstrates the dismissive attitude shown by an elected member of Halston Street Credit Union towards my Office. This uncooperative approach by the Halston Street Credit Union was disappointing and unacceptable. Thankfully my staff do not encounter such attitudes every day and, in the event, the staff and manager in the Credit Union were very co-operative to my authorised officers during their visit. Our approach to complaints, as provided under the Acts, is to try to reach an amicable resolution by engaging openly and honestly with the parties concerned. When a data controller fails to cooperate satisfactorily with an investigation conducted by my Office, I will use my legal powers without hesitation, as this case demonstrates. Neither I nor my staff will be deterred from taking the actions that we consider necessary.

As I reflect on this regrettable and time-consuming incident, I note that it comes down to the Credit Union's refusal to respond to a person with a genuine complaint. The complaint was well-grounded and reasonable and, if the Credit Union had demonstrated even a basic level of customer service, the matter would have been resolved quickly and without consuming the resources of my Office. In this respect, I accept that a Credit Union has a right to trace the location of a person with whom it needs to communicate for a genuine business reason and using reasonable means. For this reason I have no difficulty with the sending of the initial letter.

Case study 15: Tesco and the resale of an Apple ipod containing a customer's personal data

In March 2008 I received a complaint from a data subject regarding the resale by a Tesco store of an Apple ipod which she had returned to the store after it developed a fault and onto which personal data relating to her had been downloaded.

The data subject informed my Office that she purchased the ipod at a Tesco store in May 2007 and that she returned it a few days later when it developed a fault. After purchasing it, the data subject had successfully downloaded music and photographs from her computer onto the ipod and she had registered it in her name. On returning the ipod she made a point of informing a member of staff at the Tesco store that due to the fault she was unable to delete from the ipod her personal photographs and music prior to returning it. She was given a replacement ipod immediately.

However, in early January 2008, the data subject became aware through an acquaintance that the ipod she had returned the previous May had subsequently been resold by Tesco to a different customer. The data subject contacted this customer who confirmed to her that she had purchased the ipod as a Christmas gift for her daughter at the same Tesco store some months after the data subject had returned it. She also informed the data subject that, on purchasing the ipod, she found that she had access to the data subject's music and personal photographs. When she tried to register the ipod in her daughter's name, it was confirmed that the ipod was still registered in the name of the data subject. That customer also returned the ipod to the Tesco store.

Understandably, the data subject was concerned to find that the faulty ipod that she had returned to Tesco in May was resold again some time later with her personal data still on it. My Office contacted Tesco's Head Office regarding this matter. Tesco subsequently acknowledged to my Office that the ipod returned by the data subject should not have been put on sale after she had returned it. It informed my Office that its own internal controls failed to operate on this occasion and that the ipod should have been returned to its supplier. Instead, it appears to have been repackaged, retained in the store for some time and then inadvertently put on sale again. Tesco

also informed my Office that when the ipod was returned a second time, its internal processes operated effectively and the ipod was returned to the supplier.

Tesco informed my Office that as a result of this incident it instituted a review of the data protection compliance processes in its stores. This included implementing more robust processes for the storage, return and tracking of any devices that contain personal data. Tesco also informed my Office that as part of its review of its data protection compliance processes, it had reiterated to its entire staff the need to be careful about how its customers' personal data is used.

During my Office's investigation of this complaint, Tesco expressed regret at the inconvenience and concern caused to the data subject as a result of the manner in which the matter was dealt with by the store. It also offered a gesture of goodwill to the data subject and expressed a wish to write directly to her to express its apologies for the incident.

As the Data Protection Acts mandate my Office, in the first instance, to resolve complaints amicably between the parties concerned, my Office informed the data subject of Tesco's interest in reaching an amicable resolution. The data subject accepted Tesco's goodwill gesture and letter of apology, both of which were forwarded to her via my Office.

This case perfectly demonstrates circumstances when, through the intervention of my Office, a data controller is made aware that it has breached the Acts and is reminded of its obligations under the Acts. At the same time, the concerns of a data subject are addressed and the matter is resolved amicably between the parties. It also highlights the need for retailers to raise awareness among their staff about the capacity of portable devices which they sell in their stores to process and retain personal data. Robust procedures are necessary in retail outlets to prevent incidents of a nature similar to that outlined in this case.

Case study 16: Failure to properly safeguard a staff member's medical certificate

My Office received a complaint from a solicitor on behalf of a data subject whose personal information, contained in a medical certificate, had been accessed in an unauthorised manner while in the possession of her employer.

The data subject was employed by a catering company that had a contract to provide services to the Defence Forces. It was brought to her attention by a member of the Defence Forces that her medical certificate was displayed on a notice board in the office of a Unit Manager in the catering company. This office was shared with a member of the Defence Forces.

Upon receipt of the complaint, my Office contacted the catering company and requested that the medical certificate be removed from the notice board immediately. We also advised the company that a medical certificate, which reveals the health status of a person, is sensitive personal data under the Data Protection Acts. We informed them that, from the information supplied by the data subject, it appeared likely that appropriate security measures were not in place to prevent unauthorised access to the medical certificate.

My Office received a response from the catering company outlining the findings of its investigation into the alleged breach. It explained that the Unit Manager placed the certificate on her personal notice board which hangs directly behind her desk. It was not on view at any time. It was placed behind a number of other documents on the notice board. It alleged that the third party who had accessed the certificate had entered the office without permission and would have had to deliberately seek the certificate. The company informed my Office that it takes its obligations under the Data Protection Acts very seriously and that all personal data relating to employees at any unit is the responsibility of the Unit Manager. Such data is to be held securely in locked cabinets unless required by another department within the business. The company also informed my Office that steps had been taken to remind all managers of their duties when dealing with confidential data.

The main concern for my Office was that the certificate was placed on a notice board in an unlocked office and it was clear that the Unit Manager did not adhere to the company's security procedures when handling the data subject's medical certificate. Under Section 10 of the Acts I am mandated to seek an amicable resolution of complaints. To this end my Office requested that the company submit proposals to help achieve an amicable resolution. The company subsequently proposed to make a donation to a charity of the data subject's choice and it agreed to send a letter of apology to the data subject. The data subject, through her solicitor, accepted this proposal as an amicable resolution of her complaint.

This case demonstrates well the care which data controllers must exercise in the processing of all personal data in its possession, especially sensitive personal data.

Case study 17: A web design company is requested to delete a marketing database

I received a complaint from a data subject about the receipt of an unsolicited marketing email from Matrix Internet, a company advertising website design services. Disappointingly, this was the second time that this company had come to the attention of my Office concerning marketing emails sent to the same complainant. During a previous investigation, the company had given an undertaking that the complainant's email address would be removed from its marketing database.

As a result of this complaint and given our previous encounter, my Office had serious concerns about the marketing activities of this company. We sought an immediate explanation as to how the complainant's details had remained on its marketing database. In response, the company apologised and it explained that an internal error had resulted in the email address of the complainant being listed twice on the marketing database. The company had removed only one of those entries and, as a result, the complainant had continued to receive marketing emails.

I was encouraged by the company's swift response and co-operation with my Office's investigation. However, in light of what had happened to the complainant's personal data, it was clear that it was necessary to request the company to delete its entire marketing database. I considered that this was the only certain method of protecting other individuals on the company's marketing database from exposure to the receipt of unsolicited marketing emails. The company agreed to the request to delete its marketing database. In addition, the company undertook to cease marketing activity until such time as it had put in place a more appropriate system for carrying out marketing operations and managing 'opt out' requests. After a period of three months, the company reported that it was in a position to recommence marketing activities as it had, in the intervening period, introduced a new system to ensure that its marketing systems were compliant with the requirements of data protection legislation. The complainant was satisfied with this outcome. Since then my Office has received no further complaints against this company.

This complaint resulted in the deletion, at my request, of a data controller's marketing database. In terms of remedial action to protect the public from unsolicited marketing, a request for the deletion of a marketing database is not insignificant and it can result in a large loss of marketing targets for the data controller concerned.

Case study 18: A civil summons is served on the wrong person

In February 2008 I received a complaint from a data subject who had received a District Court civil summons from a firm of Solicitors acting on behalf of a property management company. The civil summons named a male and a female as the defendants in the matter. The data subject shared the same full name as that of the male named on the summons. The data subject phoned the solicitors concerned to inform them that he did not know anything about the matter referred to on the summons, that the female named on the summons was not known to him and that she did not reside at his address. When he asked the solicitors where they had sourced his address he was told that their enquiry agent had given it to them.

My Office commenced its investigation by contacting the solicitors concerned to establish if, as alleged, the complainant had been mistakenly served with a summons which was proper to another man of the same name. The solicitors subsequently responded and confirmed that they accepted that the person who received the summons in this matter was not the person with whom their clients had contracted. They informed my Office that they had relied on information provided by an agent. They also asked my Office to convey their sincere apologies to the data subject for any inconvenience that may have been caused to him.

My Office informed the data subject of the response of the solicitors and sought his views about how his complaint against the solicitors might be resolved to his satisfaction. He indicated that this could be achieved by the data controller agreeing to cover the legal and medical costs incurred by him as a direct result of being wrongly served the civil summons. The data subject informed my Office that on receipt of the civil summons it was necessary for him to engage a solicitor to deal with the matter as he had been summoned to appear before the District Court on an appointed date. He also stated that he suffered considerable distress as a result of receiving the summons and that he had attended his doctor as a direct result. The data subject was also concerned that the summons served on him was now a matter of public record in the courts system and he said that it was incumbent on the solicitors to have this matter rectified by requesting the Courts Service to clear his good name.

The solicitors immediately indicated their willingness to resolve this matter as sought by the data subject and confirmed that there was no public record of the proceedings in this matter. In the solicitors' view, the issue arose as a direct result of the actions of its enquiry agent. For this reason, it had been agreed that the enquiry agent would make a payment directly to the data subject's solicitor in settlement of the matter and confirmed that this had taken place. Unfortunately, the enquiry agent had not made any contact with the data subject or his solicitor on this matter. Soon afterwards the solicitors sent my Office, on their own behalf, a cheque made payable to the data subject to cover the full costs incurred by him in this matter. They stated that they had been misled by the enquiry agent who had indicated that the matter had been resolved with the data subject's solicitor. They indicated that, as a result, they had dispensed with the services of the enquiry agent with immediate effect. The data subject expressed his satisfaction with the outcome and thanked my Office for helping to bring this matter, which had caused him great distress, to a satisfactory conclusion.

This case highlights the distress and inconvenience that can be caused to an innocent individual as a result of the processing of inaccurate personal data. The serving of a summons is a significant action and it can be a matter of great anxiety for an individual to receive a summons, even when that individual is not the legitimate subject of the summons. Greater care should have been taken by all involved in the process of serving this summons.

Case study 19: Personal data is disclosed in a letter

My Office received a complaint in February 2008 from a data subject stating that a letter containing personal information about him was disclosed by the HSE to a third party without his consent. The data subject was involved in a tenancy dispute with his landlord resulting in the matter being referred to the Private Residential Tenancies Board (PRTB) which is the dispute handling body for such situations. The data subject's Community Welfare Officer (CWO) was unable to attend a subsequent hearing at the PRTB and instead wrote to the solicitor acting for the data subject's landlord, outlining the position regarding the data subject's rent supplement entitlements. The CWO included a statement in the letter regarding, as he viewed them, malicious letters between the data subject and Community Welfare Office staff. This information was not related to the tenancy issue and the basis for its inclusion in this letter was not clear to my Office.

My Office contacted the HSE about this case and pointed out its obligations under the Data Protection Acts, 1988 & 2003. The HSE responded with a contention that the disclosure was proportionate. My Office did not accept this position given the nature of the dispute before the PRTB and the lack of any clear link between that dispute and the nature of the customer relationship between the data subject and the Community Welfare Office. The processing of this personal information took place without the consent of the data subject. It was clearly unnecessary for the purposes of the legitimate interests pursued by the HSE and it did not meet any of the other requirements of section 2A of the Acts. Accordingly, we informed the HSE that we considered that the disclosure of this personal information was a contravention of the Acts.

To try to reach an amicable resolution of this complaint, my Office proposed that the CWO should issue an amended version of the letter which would omit the statement referring to the nature of communications between the HSE and the data subject. We proposed that this amended letter should be issued to the solicitor concerned with a request that he should replace the original letter with the amended version. In addition, we asked the HSE to write to the PRTB to request it to replace the original letter with the amended version. The data controller agreed to this course of action

and the matter was concluded satisfactorily. **All data controllers, but especially the HSE (given the sensitive nature of its responsibilities), need to be very careful to ensure that only strictly relevant personal data is disclosed when it is necessary to discuss customers/patients with external parties**.

Case study 20: Dell and persistent unsolicited marketing faxes

The direct marketing activities of Dell resulted in a complaint to my Office during the year. The complaint concerned repeated fax messages sent by Dell to the line of a subscriber. The complainant provided my Office with a copy of a sample of the faxes he had received. From an initial examination of the complaint, there were two clear issues of concern. In the first place, the fax number of the complainant was registered on the NDD opt-out register. Secondly, the complainant's numerous attempts to opt-out of receiving fax messages from Dell using the fax number provided by the company had failed because the number provided appeared to be out of service. As a result, he continued to receive unsolicited marketing fax messages.

My Office contacted Dell and requested an explanation. Dell acknowledged that eight fax messages had been sent to the individual. Regarding the inability of the complainant to 'opt out', Dell acknowledged that an internal error resulted in an incorrect digit being inserted in the 'faxback' number printed on the fax messages sent to the complainant. Regarding the inclusion of the complainant's fax machine number on the NDD opt-out register, Dell advised that the complainant's number was supplied to it by a third party provider. That list was then sent to its fax marketer for checking against the NDD. Dell stated that the fax marketer advised it that the complainant's number was not listed on the NDD at the time when the fax messages were issued. However, my Office's investigation confirmed that the complainant's number had been listed on the NDD since 2007.

Following the intervention of my Office, Dell agreed to take a number of corrective measures to address the shortfalls in its fax marketing operations, including deletion of the complainant's number from its marketing database. Dell also indicated that it wished to attempt to resolve the complaint by amicable resolution. In that context, as a goodwill gesture, Dell offered laptop equipment to the value of €2,500 to a charity of the complainant's choice. It also communicated a letter of apology to the complainant and an undertaking that he would not receive any further marketing from Dell unless he specifically requested such information. The complainant was happy to have his complaint resolved on this basis.

This complaint demonstrates the need for any data controller engaged in direct marketing by post, fax, email or text message to have appropriate procedures in place to ensure that it meets the requirements of the law in this area. In particular, a valid facility to opt-out must be provided and must be working.

Case study 21: Access is wrongly denied in respect of an accident report

I received a complaint from a data subject who had been involved in an accident at work. The data subject had made an access request, under section 4 of the Data Protection Acts, to their employer for a copy of all information held about them, including the accident report form. The employer had not responded to the request within the forty day timeframe specified in section 4 of the Acts.

My Office contacted the data controller to enforce compliance with the terms of the access request. The data controller stated that they had passed the request on to their insurance company who were dealing with legal proceedings arising from the accident. My Office pointed out that the obligation to comply with an access request was on the data controller and not on the insurance company. My Office informed the data controller that we were investigating its failure to respond to an access request.

The data controller then provided certain documents containing personal data to the data subject. However, it failed to provide a copy of the accident report form.

My Office contacted the data controller again to request that the outstanding documents be furnished to the data subject. The data controller responded by claiming a restriction on the right of access under section 5(1)(g) of the Acts based on an assertion that the documents were exempt from disclosure due to legal privilege. This provision restricts the right of access with regard to personal data in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his professional legal advisers or between those advisers.

My Office rejected this claim because in this case the accident report was prepared on foot of the legal requirement for an accident report to be created if a workplace injury results in at least three days absence from work. This is set out in Regulation 59 of Statutory Instrument No. 44 of 1993. My Office also rejected claims by the data controller that, as the accident report form was created with the assistance of their legal adviser, it could be withheld on the basis of legal privilege. As a result, the data controller provided a copy of the accident report form to the data subject.

While the Data Protection Acts provide for limited, narrow restrictions to the right of access by a data subject to their personal data, this case highlights the fact that my Office will rigorously examine complaints of this nature to establish whether the restriction asserted by a data controller can be legitimately relied upon.

Part 3

Guidance

Guidance note for data controllers on keeping personal data obtained from the electoral register up-to-date

The following guidance note has been prepared as an aid to data controllers in the practical application of the obligation to keep personal data up-to-date as it applies to personal data which is sourced from the Electoral Register.

Since 2004, electoral registration authorities are required to publish two versions of the Electoral Register – the 'Full Register' and the 'Edited Register.'

> The 'Full Register' lists everyone who is entitled to vote and it can only be used for an electoral or other statutory purpose.
>
> The 'Edited Register' contains the names and addresses of people whose details can be used for a purpose other than an electoral or other statutory purpose, for example for direct marketing use by a commercial organisation.

It is an offence under section 13A(3) of the Electoral Act, 1992 (as amended by the Electoral (Amendment) Act, 2001) to use information on the Full Register for non-electoral or non-statutory purposes. Data controllers may only process personal details published on the Edited Register for non-electoral and non-statutory purposes.

Section 2(1)(b) of the Data Protection Acts, 1988 & 2003 places a statutory obligation on data controllers to ensure that personal data kept by them shall be accurate, complete and up-to-date. There is a statutory obligation on data controllers to ensure that personal data obtained from electoral registers published prior to the introduction of the Full Register and the Edited Register in 2004 is kept up-to-date.

The Data Protection Commissioner acknowledges that a period of adjustment was required for data controllers in the marketing sector following the changes introduced to the Electoral Register in 2004. That period of adjustment has long since passed. It is the view of the Data Protection Commissioner that data controllers have had ample

time since 2004 to update their records and to ensure that individuals whose details have not been published in the Edited Register are removed from databases which are used for non-electoral or non-statutory purposes. By now, data controllers who process personal data obtained from the electoral register must have a system in place to update their records to take account of the new Edited Register which is published each year.

In addition, individuals whose details have not been published on the Edited Register must be presumed not to have consented to their personal data being used for direct marketing purposes. Accordingly, any use of the personal data of those individuals for direct marketing constitutes a breach of the Data Protection Acts.

In summary, if a data controller uses databases holding personal data gleaned solely from electoral registers at any time, that data controller has a statutory obligation to ensure that such databases no longer contain personal data that is not published on the most up-to-date version of the Edited Electoral Register. This obligation requires a data controller to undertake an annual updating exercise.

Guidance note for data controllers on purpose limitation and retention in relation to credit/debit/charge card transactions

The following guidance has been prepared as an aid to data controllers (http://www.dataprotection.ie/docs/Are_you_a_Data_Controller?/43.htm) who process credit/debit/charge or other relevant card payments regarding the practical application of section 2(1)(c) of the Data Protection Acts 1988 & 2003 (http://www.dataprotection.ie/viewdoc.asp?DocID=796&ad=1) . Section 2(1)(c) requires data controllers to comply with the following provisions concerning personal data kept by them:

- the data shall have been obtained for one or more specified, explicit and lawful purpose(s);
- the data shall not be further processed in a manner incompatible with that purpose or those purposes;
- the data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed; and
- the data shall not be kept for longer than is necessary for that purpose or those purposes.

Specific, explicit and lawful purposes

Data controllers (http://www.dataprotection.ie/docs/Are_you_a_Data_Controller?/43.htm) who obtain personal data (http://www.dataprotection.ie/viewdoc.asp?DocID=210) from a data subject may do so for one or more specific, lawful and clearly stated purposes. When personal data stored on a card is collected for the purposes of a transaction, it can be assumed that the purpose for its collection ends following completion of the payment for a product or service.

Further processing

Data controllers who obtain personal information for one or more legitimate purposes may not use that data for any other purpose except in ways which are compatible with the original purpose(s). Personal data obtained from a card for a particular transaction cannot be used subsequently for other transactions without express consent to do so. Any use of the data without such consent would breach the 'fair obtaining' rule as set

out in the Data Protection Acts. To meet this obligation, data controllers are advised to put in place appropriate data deletion procedures and security measures to ensure that information obtained for one purpose may not be accessed and used for another purpose. Prior to the termination of the customer relationship, if the customer has clearly opted-in (as opposed to not having opted-out) to their data being retained for future transactions, this would permit further processing (for example, further processing is permissible if a customer has consented to having their personal data retained for ease of retrieval for future transactions).

Adequate, relevant and not excessive

Personal data sought and kept by data controllers should be sufficient to enable them to achieve their specified purpose(s) and no more than that. There is no basis for data controllers to collect or keep personal data that they do not need 'just in case' a use might be found for it at a future date.

Retention

Data controllers must be clear about the length of time during which personal data will be kept and the reasons why the information is being retained for this period. When the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner. It is the view of this Office that personal data obtained from a card should only be retained for a period of 13 months (at most) to allow for copy voucher requests. This applies only in cases where the customer has had to sign a receipt for their transaction to be processed. In these cases, the information should be retained separately and solely for the purpose of previous payment queries. It should not be used for future transactions or any other purposes. In the case of card transactions processed using Chip and PIN (EMV) technology, it is not necessary for vendors (data controllers) to hold onto the receipts at all, as the electronic record is available directly from the cardholder's card issuer.

Appendices

Appendix 1 – Presentations

Appendix 2 – Registration statistics

Appendix 3 – Account of income and expenditure

Appendix 1 – Presentations and Talks

During 2008 my staff and I gave presentations to the following organisations:

Citizens' Advice

Citizens' Information (Information Providers Programme) (x3)

Educational

CBS Portlaoise (x2)

Department of Education and Science Curriculum Development Unit (x3)

DIT

Irish Computer Society

Scoil Chríost Rí

Trinity College (x2)

Financial Services

ACCA Sligo

Credit Union Managers Association – CUMA

Other Commercial

Kilkenny County Enterprise Board

PharmaChemical Ireland Security Group

Government Agencies

CAAB Annual Conference

Czech Delegation

Department of Foreign Affairs

Public Affairs Ireland (x2)

Public Sector Equality Learning Network

Probation Service

Pobal

Information Commissioner of Slovenia

Institute of Public Administration (x2)

Oireachtas (x2)

Telecommunication Sector

Telecommunications and Internet Federation (IBEC)

Health Sector

Beaumont Hospital

IPPOSI Patient Registries Meeting

Irish Association of Cardiac Rehabilitation (IACR)

Insurance Sector

Integrated Governance, Risk and Compliance

Insurance Institute of Ireland

Life Insurance Association (L.I.A)

International

EC Commission – Slovenia

Future of Trust in Computing Conference

Legal Sector

Chief State Solicitor's Office

Limerick Bar Association

Local Authorities

Dublin City Council

Local Government FOI Officers Network

Motor Tax Office Conference Laois County Council

Mixed Seminars

ADAPT

CIF

Data Protection Forum, London

Data Protection Fundamentals

Data Protection Roadshow

ICS Privacy Forum

IPA

PAI

IIR – IBC

Institute of International and European Affairs

Irish Council for Bioethics

Irish Society for European Law

Oracle/IBEC/Deloitte

Privacy & Data Protection

Robert Walters Recruitment Consultancy

Transatlantic Events

Voluntary/Charity

Tullamore Business and Professional Women's Club

Appendix 2 - REGISTRATIONS 2008

The total number of register entries in 2008 was 4,156. This figure can be broken down into the following categories:

(a) Financial and Credit Institutions

516

(b) Insurance Organisations

455

(c) Persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts

123

(d) Telecommunications/Internet access providers

57

(e) Health Sector

1202

(f) Pharmacists

1001

(g) Miscellaneous

450

(h) Data Processors

352

Total number of registration entries:

2006	**2007**	**2008**
6380	**5699**	**4156**

In 2008 the number of organisations registered decreased by 1,543 or 27%. This decrease reflects the implementation of new registration regulations (S.I. No. 657 of 2007) on 1 October 2007. Changes in the requirement to register in the education and legal sectors contributed most to the decrease.

Appendix 3 - Abstract of Receipts and Payments in the year ended 31 December 2008*

	2007 €	2008 €
Receipts		
Moneys provided by the Oireachtas	1,835,154	2,041,097
Registration Fees	533,123	591,421
	2,368,277	2,632,518
Payments		
Staff Costs	1,297,809	1,399,075
Establishment Costs	269,720	184,460
Education and Awareness	158,587	97,712
Legal and Professional Fees	61,497	323,311
Incidental and Miscellaneous	47,541	36,539
	1,835,154	2,041,097
Payments of Fees to the Vote for the Office of the ` Minister of Justice, Equality and Law Reform	533,123	591,421
	2,368,277	2,632,518

**The financial statements of the Office are subject to audit by the Comptroller and Auditor General and after audit are presented to the Minister for Justice, Equality and Law Reform for presentation to the Oireachtas.*